APPENDIX C

Johnny 2 User Test Details

C.1 Description of Test Participants

Effort were taken to parallel Whitten and Tygar's recruitment and testings effort from the original *Johnny* experiment as closely as possible given the expanded goals of *Johnny 2*. This includes the use of similar language, posters, subject compensation, pre-test, consent forms, and after-test debriefing whenever possible.

C.1.1 Recruitment

Subjects were recruited with an email sent to the mailing list `free-money@mit.edu` (a mailing list of people who like to earn money by volunteering for human subject testing) and by posting 75 posters throughout the halls of MIT. Approximately 85 people responded to the advertisement.

By design, recruitment language was virtually identical to those used by Whitten and Tygar. For example, Figure C-1 shows the recruitment text that was used in the *Johnny* experiment, while Figure C-2 shows the recruitment poster used in *Johnny 2*.

> Earn $20 and help make computer security better!
>
> I need people to help me test a computer security program to see how easy it is to use. The test takes about 2 hours, and should be fun to do.
>
> If you are interested and you know how to use email (no knowledge of computer security required), then call Alma Whitten at 268-3060 or email alma@cs.cmu.edu.

Figure C-1: Alma Whitten's recruitment poster, from [Whi04a, p.93]

Earn $20 and help make computer security better!

I need people to help me test a computer security program to see how easy it is to use. The test takes about 1 hour, and should be fun to do.

If you are interested and you know how to use email (no knowledge of computer security required), then call Simson at 617-876-6111 or email simsong@mit.edu

$20 Security Study
Simson
617-876-6111
simsong@mit.edu

$20 Security Study
Simson
617-876-6111
simsong@mit.edu

$20 Security Study
Simson
617-876-6111
simsong@mit.edu

$20 Security Study
Simson
617-876-6111
simsong@mit.edu

$20 Security Study
Simson
617-876-6111
simsong@mit.edu

$20 Security Study
Simson
617-876-6111
simsong@mit.edu

$20 Security Study
Simson
617-876-6111
simsong@mit.edu

Figure C-2: The poster used to recruit subjects; 75 copies were placed on first-floor hallways in MIT buildings 26, 8, 6, 2, 4, 10, 7 and 5

Thank you for your interest in participating in the testing! Here is the intake questionnaire. The answers will be used to select a set of test participants that has the particular demographic characteristics needed for this research study. All information you give will be kept private, and will only be included in research results in anonymized form.

1. How old are you?
2. What is your highest education level (high school, some college, undergrad degree, some grad school, grad degree)?
3. What is your profession or main area of expertise (for example arts, science, medicine, business, engineering, computers, administration...)?
4. For how long have you been using electronic mail?
5. Have you ever studied number theory or cryptography?
6. Have you ever used security software, such as secure email in Netscape or Microsoft Outlook, or PGP, or any other software that involved data encryption? If yes, what was the name of that software?
7. Do you know the difference between public (asymmetric) key cryptography and private (symmetric) key cryptography? If yes, please explain briefly.
8. How do you read your email? (What program or online service?)
9. How did you hear about this study?

Thanks again, and I look forward to hearing from you.

Figure C-3: The Participant Intake Questionnaire.

C.1.2 Participant intake questionnaire

As mentioned in Section C.1.1, approximately 85 people responded to the advertisements for the study. Each of these individuals was sent a copy of the Participant Intake Questionnaire (Figure C-3) to disqualify those who had some knowledge of public key cryptography. Of those responding to the questionnaire, 28 were disqualified because they were familiar with public key cryptography, PGP, or S/MIME. These respondents were sent a message similar to the one in Figure C-4 and scheduled on a first-come, first-serve basis. Those that were excluded were sent a message similar to the one in Figure C-5. We were pleased that the respondents represented a wide range of age, education level, and work experience.

A total of 44 subjects were tested under the terms of the COUHES protocol, with data from one subject (S13) being discarded. (S13 was the first subject to experience the Briefing intervention. Based on feedback from S13, the briefing was changing, making it inappropriate for S13's data to be included in the overall results.)

Subjects ranged in age from 18 to 63 ($\overline{x} = 33; \sigma = 14.2$) The participants had all attended at least some college; 21 were either graduate students or had already earned an advanced degree. Professions were diverse, including PhD candidates in engineering and biology, administrative assistants, clerks, and even a specialist in import/export. Two of the subjects (S12 and S19) appeared to have significant difficulty understanding the English messages in the test, although they were nevertheless able to complete the experiment.

Hi. You fit the demographics that I'm looking for!

The study takes between 20-60 minutes and happens in my office on the 8th floor of the MIT Stata Center.

Directions on how to get to my office are at http://www.simson.net/g828/

I keep an online calendar at http://calendar.simson.net/

Right now following slots are available; do any work for you?

Wednesday, January 26th, 1pm - 2pm
Wednesday, January 26th, 2:15pm - 3:15pm
Thursday, January 27th, 5:00pm - 6:00pm
Friday, January 28, 3:15pm - 4:15pm
Friday, January 28, 4:30pm - 5:30pm

Simson Garfinkel
simsong@csail.mit.edu

Figure C-4: Message sent to qualifying subjects

Hi. Thanks again for responding to the poster and the survey.

Unfortunately, right now I have enough people in your particular demographic category, so I don't need you as a subject.

This might change in the future. If you wish, I can hold your information on file and get back to you if things change.

-Simson Garfinkel
simsong@csail.mit.edu

Figure C-5: Message sent to disqualified subjects

C.2 Description of the Testing Process

C.2.1 Test environment

Testing took place in MIT Room 32-G828, an 8th floor office in the MIT Stata Center. Figure C-6 shows a floor plan of the testing room; figures C-7 and C-8 photographs of the experimental setup and a view of the experimenter's laptop from the subject's chair, respectively.

C.2.2 Greeting and orientation

Consent forms approved by the MIT Committee On the Use of Humans as Experimental Subjects (COUHES) appears in Figures C-10 on page 387 through C-13 on page 390. The Initial Task Description for the **NoColor** and **Color** group appears in Figure C-14 on page 391, while the Initial

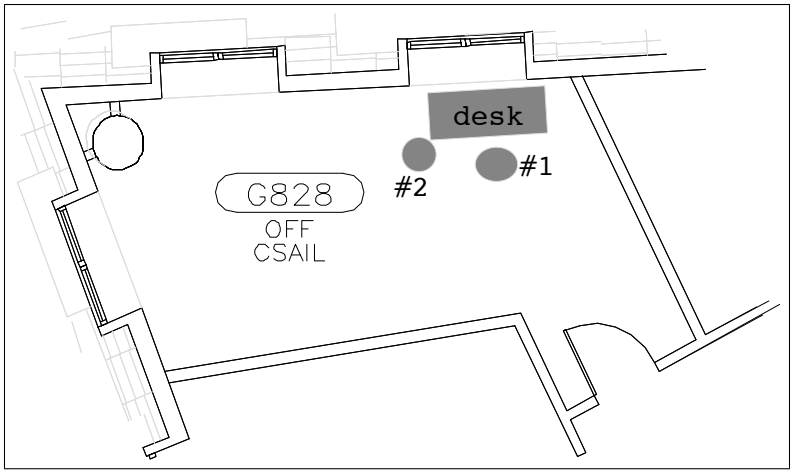

Figure C-6: The floor plan of 32-G828 showing the location of the Johnny 2 testing desk (grey rectangle) the subject's chair (oval #1) and the experimenter's chair (oval #2). (Excerpted from [MIT04], with modifications.)

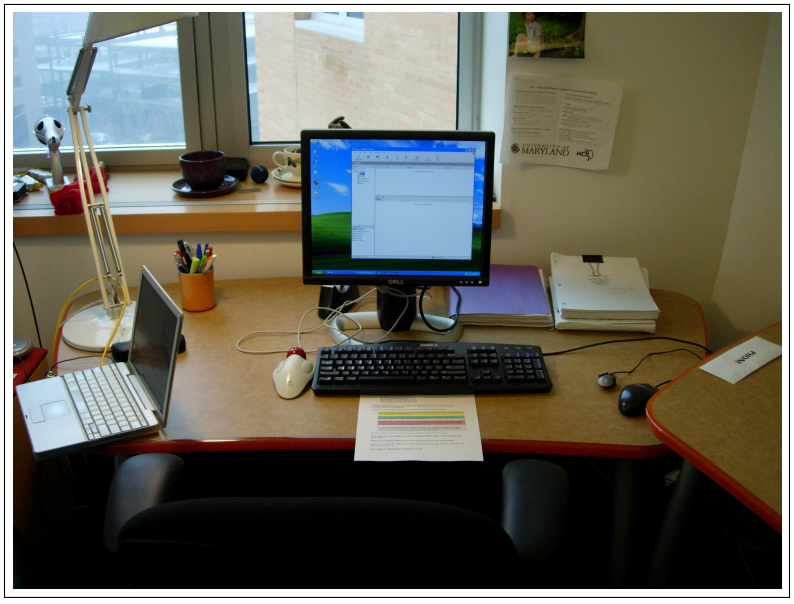

Figure C-7: A photograph of the Johnny 2 experimental station. The experimenter's laptop is visible on the left. In front of the keyboard is the Johnny 2 **Color+Briefing** Handout. At the right is the "PHONE" (Figure C-9).

Figure C-8: A view of the experimenter's laptop from the experimental subject's chair. Note that the laptop's screen is not visible.

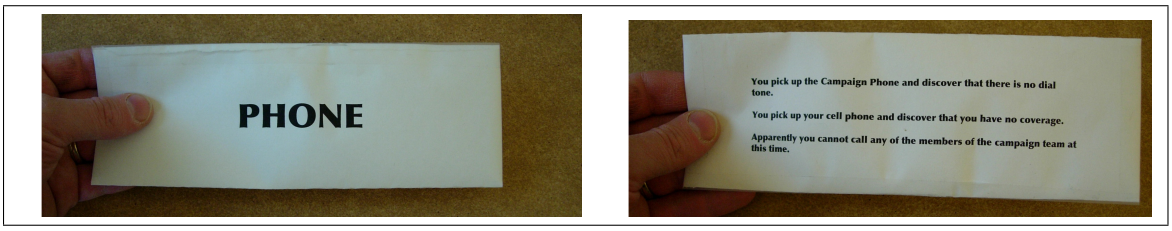

Figure C-9: The front and back of the Johnny 2 "PHONE". The text reads: "You pick up the Campaign Phone and discover that there is no dial tone. / You pick up your cell phone and discover that you have no coverage. / Apparently you cannot call any of the members of the campaign team at this time."

Task Description used by the **Color+Briefing** group appears in Figure C-15 on page 392.

C.2.3 Testing

The test began when the experimenter pressed the "Send email #1" button on the Experimenter's work bench (see Figure 7-7 on page 262). This sent message #1 to the subject. Subjects who did not do so were prompted to press the Outlook Express 'Send/Recv" button to receive the message.

A copy of Camtasia Studio 2 running on the subject's computer recorded the subject's screen and the subject's spoken utterances. Subjects who were quiet were reminded "it would be helpful if you could think out loud."

The experimenter used a Macintosh laptop both to take notes and to advance the experiment by pressing the numbered buttons on the Experimenter's work bench.

Unlike in the original *Johnny* experiment, subjects were only sent the scripted messages that has

CONSENT TO PARTICIPATE IN NON-BIOMEDICAL RESEARCH

Johnny 2:
A Study of Email Security

You are asked to participate in a research study conducted by Simson L. Garfinkel, MS, and Robert C. Miller, Ph.D. at the Massachusetts Institute of Technology (M.I.T.). This research will be used as part of Simson L. Garfinkel's Ph.D. dissertation. You were selected as a possible participant in this study because you responded to our advertisement and you did not have prior experience with mail security technology. You should read the information below, and ask questions about anything you do not understand, before deciding whether or not to participate.

- **PARTICIPATION AND WITHDRAWAL**

Your participation in this study is completely voluntary and you are free to choose whether to be in it or not. If you choose to be in this study, you may subsequently withdraw from it at any time without penalty or consequences of any kind. The investigator may withdraw you from this research if circumstances arise which warrant doing so.

- **PURPOSE OF THE STUDY**

This study is to test the design of Outlook Express and CoPilot, a program that we have written to help sending and receiving secure email with Outlook Express. We are interested in seeing how you use CoPilot and what your reactions are to the program.

- **PROCEDURES**

If you volunteer to participate in this study, we would ask you to do the following things:

If you can manage it, it is extremely useful to me if you "think aloud" during the test. The computer has a microphone that will pick up what you say, and I'll be taking notes as well. The more informative you can be about what you are doing and thinking, the better my data will be.

In the test, you will be asked to play the role of a volunteer in a political campaign. After you volunteered, you were given the role of Campaign Coordinator. Your task is to send updates about the campaign plan out to the members of the campaign team by email. It is very important that the plan updates be kept secret from everyone other than the members of the campaign team, and also that the team members can be sure that the updates they receive haven't been forged. In order to ensure this, you and the other team members will need to use CoPilot to make sure that all of the email messages are secure.

Your email address for the purpose of this test is ccord@campaign.ex.com, and your password is **volnteer**.[1] You should use the title "Campaign Coordinator" rather than using your own name.

[1] Please note that the word "volnteer" is intentionally misspelled.

Figure C-10: Page 1 of the consent form

Outlook Express and CoPilot have both been installed, and Outlook Express has been set up to access the email account. No manuals for these programs are provided, but there may be some online help. A pad of paper and pens are also provided, if you want to use them.

Before we start the test itself, I'll be giving you a very basic demonstration of how to use Outlook Express to send and receive mail. The goal is to have you start out the test as a person who already knows how to use Outlook Express to send and receive email, and who is just now going to start using CoPilot to make sure your email can't be forged or spied on while it's being delivered over the network. The Outlook Express tutorial will take about 5 minutes, and then we'll begin the actual testing. ~~You can also use Mozilla Thunderbird if you would prefer, but not all of the advanced features of CoPilot work with Mozilla.~~

The actual test itself should take roughly 20 minutes.

After the test, you will be asked to answer a brief questionnaire with five questions.

- **POTENTIAL RISKS AND DISCOMFORTS**

There are no known or foreseeable risks associated with participation in this study.

- **POTENTIAL BENEFITS**

By partaking in this test, you may learn more about the features of Microsoft Outlook Express and/or secure email.

This research is designed to help researchers develop techniques for making computer security systems easier-to-use. We hope that your participation will help in this effort.

- **PAYMENT FOR PARTICIPATION**

You will be paid $20 at the end of this experiment. If you decide to withdraw from the experiment before it is over, you will receive $1 for every 5 minutes of the experiment that have elapsed.

- **CONFIDENTIALITY**

Any information that is obtained in connection with this study and that can be identified with you will remain confidential and will be disclosed only with your permission or as required by law.

The notes that the experimenter takes will not be matched with any of your personal information, such as your name, email address, or phone.

This test will be recorded to assist in the writing of the research report. The recording will consist of an audio recording of your comments and a recording of the computer's screen made with special screen-recording software. If you wish, you may review the recording at the conclusion of the experiment. This recording will be used for creating a transcript of your test. Only members of the research team will have access to the recording. The recording will be on a secure computer. The audio recording itself will not be published or redistributed in any way, and will be destroyed at the conclusion of this experiment and the publication of the results. We may use the

Figure C-11: Page 2 of the consent form

screen recording in our publications, but it will not have any information that personally-identifies you.

Each participant in the experiment will be given a code, such as Q1, Q2, Q3, etc. This code will be used to label experimenter's notes and the recording associated with the test. The codes will also be used in all publications resulting from today's test.

- **IDENTIFICATION OF INVESTIGATORS**

If you have any questions or concerns about the research, please feel free to contact

Principal Investigator:	Simson L. Garfinkel simsong@mit.edu 32-G804 617-876-6111
Faculty Sponsor:	Robert C. Miller rcm@mit.edu 32-G716 617-324-6028

- **EMERGENCY CARE AND COMPENSATION FOR INJURY**

In the unlikely event of physical injury resulting from participation in this research you may receive medical treatment from the M.I.T. Medical Department, including emergency treatment and follow-up care as needed. Your insurance carrier may be billed for the cost of such treatment. M.I.T. does not provide any other form of compensation for injury. Moreover, in either providing or making such medical care available it does not imply the injury is the fault of the investigator. Further information may be obtained by calling the MIT Insurance and Legal Affairs Office at 1-617-253 2822.

- **RIGHTS OF RESEARCH SUBJECTS**

You are not waiving any legal claims, rights or remedies because of your participation in this research study. If you feel you have been treated unfairly, or you have questions regarding your rights as a research subject, you may contact the Chairman of the Committee on the Use of Humans as Experimental Subjects, M.I.T., Room E32-335, 77 Massachusetts Ave, Cambridge, MA 02139, phone 1-617-253 6787.

Figure C-12: Page 3 of the consent form

SIGNATURE OF RESEARCH SUBJECT OR LEGAL REPRESENTATIVE

I understand the procedures described above. My questions have been answered to my satisfaction, and I agree to participate in this study. I have been given a copy of this form.

_____
Name of Subject

_____
Name of Legal Representative (if applicable)

_____ _____
Signature of Subject or Legal Representative Date

SIGNATURE OF INVESTIGATOR

In my judgment the subject is voluntarily and knowingly giving informed consent and possesses the legal capacity to give informed consent to participate in this research study.

_____ _____
Signature of Investigator Date

Figure C-13: Page 4 of the consent form

Page 1 of 2 Date _____
Subject #: _____ Printed 1/12/2005 2:55 PM

Initial Task Description

You are the campaign coordinator.

You are working for the campaign manager, Maria Page, mpage@campaign.ex.com

The other members of the campaign team are:

Paul Butler, butler@campaign.ex.com
Ben Donnelly, bend@campaign.ex.com
Sarah Carson, carson@campaign.ex.com
Dana McIntyre, dmi@campaign.ex.com

NOTE: Digital IDs for Paul, Ben, Sarah and Dana have been pre-loaded onto your machine by the IT Coordinator.

You have arrived early for work. No one else from the campaign is in the office.

If you wish to use the telephone to call a campaign member, please ask the experimenter for a "phone."

When you are asked by Maria, please send the schedule to the other team members.

Once you have done this, wait for any email responses from the team members, and follow any directions they give you.

Don't forget to "think aloud" as much as you can.

1

Figure C-14: Initial Task Description (**NoColor** and **Color**)

Page 1 of 2 Date _____
Subject #: _____ Printed 1/12/2005 2:55 PM

Initial Task Description

You are the campaign coordinator.

You are working for the campaign manager, Maria Page, mpage@campaign.ex.com

The other members of the campaign team are:

Paul Butler, butler@campaign.ex.com
Ben Donnelly, bend@campaign.ex.com
Sarah Carson, carson@campaign.ex.com
Dana McIntyre, dmi@campaign.ex.com

NOTE: Digital IDs for Paul, Ben, Sarah and Dana have been pre-loaded onto your machine by the IT Coordinator.

Digital IDs allow Outlook Express to authenticate the sender of email messages.

A Yellow Border will appear around an email message the first time a particular Digital ID is used with an email address.

A Green Border will appear around an email message each successive time that a particular Digital ID is used with an email address.

A Red Border will appear around an email message if the Digital ID used with that email address changes. This might indicate that the sender has moved to a different computer, or that someone else is trying to impersonate the sender.

A Gray Border indicates that no Digital ID was used to send the message. The sender might have forgotten or have a computer problem. Alternatively, the message might be sent by someone else who is trying to impersonate the sender.

You have arrived early for work. No one else from the campaign is in the office.

If you wish to use the telephone to call a campaign member, please ask the experimenter for a "phone."

When you are asked by Maria, please send the schedule to the other team members.

Once you have done this, wait for any email responses from the team members, and follow any directions they give you.

Don't forget to "think aloud" as much as you can.

1

Figure C-15: Initial Task Description (**Color+Briefing**)

been previously drafted: no spontaneous messages were sent from the experimenter to the subject. Subjects were permitted to ask questions to the experimenter during the test. Questions about Outlook Express (other than OE's handling of digital certificates) were generally answered, but whenever a question regarding digital certificates or CoPilot were asked, the experimenter responded "I don't know" or with a confused shrug of the shoulders.

C.2.4 Messages sent to subjects

Subjects were sent a series of eight messages, reprinted below. In each case subjects were allowed to read, evaluate, and respond to the messages before the follow-up message was sent. On occasion subjects said that they were going to ignore a message. In these cases, a period of one or two minutes was allowed to pass before next message was sent; in some cases, the subject changed their mind during this time period and decided to respond to a spoof message because they had reconsidered.

Message #1
From: Maria Page <mpage@campaign.ex.com>
To: Campaign Coordinator <ccord@campaign.ex.com>
Subject: Welcome to the Campaign! Signed: Yes; Digital ID 3400
CoPilot Color: Yellow
Text: Dear Campaign Coordinator,

Please click "reply" and send me a brief email message when you read this to let me know you are ready.

Hi there! Once again, I wanted to thank you for taking time out of your busy schedule to work with us here on the Senator's re-election campaign. It's just a few weeks to go before the election and we really, really, *really* can use your help!

I've cc'ed the other team members on this email. They are:

- **Paul Butler** `butler@campaign.ex.com`, our campaign finance manager and chief election strategiest.
- **Ben Donnelly** `bend@campaign.ex.com`, who is officially Paul's assistant, but who also runs the IT for our campaign. Ben's also a full-time student at the University of Pennsylvania.
- **Sarah Carson** `carson@campaign.ex.com`, who is a full-time graphics designer. She designed that slick bumper sticker that is on the back of your car! She also does all of our press releases.
- **Dana McIntyre** `dmi@campaign.ex.com`, who is our office manager. Normally Dana would be there with you in the office, but she's out this week because her husband is having surgery! (Don't worry, it's a routine procedure.)

Because Dana is out of the office this week, we're going to be relying on you to help out in a big way! Don't be nervous, but we are counting on you!

Please click "reply" and send me a brief email message when you read this to let me know you are ready.

—Maria

Comment: This is the initial message from Maria to the Campaign Coordinator. The message displays as yellow because it is the first message received from the email address mpage@campaign.ex.com. Maria cc's the other

campaign members on the email—Paul Butler, Ben Donnelly, Sarah Carson, and Dana McIntyre. CoPilot running on Maria's computer detects the CC and automatically includes the S/MIME certificates for each of these identities. Because this feature of CoPilot was not operational, the copy of Outlook Express running on Maria's computer had these S/MIME certificates pre-loaded. Subject's initial briefing also said that Digital IDs for these individuals had been pre-loaded onto the Campaign Coordinator's computer by the IT Coordinator.

Message #2
From: Maria Page <mpage@campaign.ex.com>
To: Campaign Coordinator <ccord@campaign.ex.com>
Subject: Speaking dates for Pennsylvania Signed: Yes; Digital ID 3400
CoPilot Color: Green
Text: 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
  - 10:00am - Toxic workshop at Pittsburgh Airport.
  - 2:00pm - Meet the workers at the docks.

It's important that we get this information out to the other members of the campaign. **But we are not releasing this information to the public until the day of each event.** If the opposing campaign discovers our schedule, they will arrange to have protesters show up at our events! That would be *really, really bad*.

Indeed, the other campaign may be trying to steal this information!

I'm having a problem with my email right now.

Please send the schedule to Paul Butler `butler@campaign.ex.com` and Dana McIntyre `dmi@campaign.ex.com`. Thanks!

Remember, if *anybody on our team* asks for a copy of the schedule, please send it out to them! But please don't send it to anyone else.

—Maria

Comment: This is the second message from Maria to the Campaign Coordinator. The message displays in green because it is the second message received from the email address mpage@campaign.ex.com. This message contains the "secret" that must be distributed to the other campaign members and simultaneously shielded from the attackers. In this message Maria asks that the Campaign Coordinator send the secret to butler@campaign.ex.com and to demi@campaign.ex.com.

Message #3

From: Ben Donnelly <bend@campaign.ex.com>
To: Campaign Coordinator <ccord@campaign.ex.com>
Subject: I need a copy of the Pennsylvania dates! Signed: Yes; Digital ID 4159
CoPilot Color: Green
Text: Dear Campaign Coordinator,

Hi! This is Ben Donnelly. I run the computer systems for the campaign. I'm also a full-time student at Penn. Welcome on board!

I just got off the phone with Maria. She said that you have a copy of the speaking dates for Pennsylvania and that you could email them to me.

Can you please email me the schedule? I'm trying to make sure that we will be able to coordinate wireless Internet coverage at each of the stops.

Thanks.

—bend

Comment: This is the first message from Ben Donnelly. It is green, however, because it the Digital ID was installed on the computer by the Campaign IT Coordinator and because Maria has previously sent Ben's key to the Campaign Coordinator. Thus, the key arrived from two trusted sources. In this message Ben asks for a copy of the schedule. Since it really is from Ben, the Campaign Coordinator should send the secret.

Message #4
From: Paul J. Butler <butler@campaign.ex.com[1]>
To: Campaign Coordinator <ccord@campaign.ex.com>
Subject: Something is wrong with my email! Signed: Yes; Digital ID 9950
CoPilot Color: Red
Text: Dear Campaign Coordinator,

Did you get my previous email? Something screwy is going on. I sent you a long message and it bounced... Did you get it?

Anyway, it's **urgent** that I get a copy of the Candidate's schedule within the next half-hour—I'm about to sign a deal with a major outdoor advertising company.

I need you to send me a copy of the candidate's schedule to **both** this account **and** my Hotmail account? You can find the address in the campaign phone book—use `Paul_J_Butler@Hotmail.com`.

Thanks!

Comment: This is the first attack message. The attacker uses a self-signed certificate which necessarily has a different ID than the ID that was passed to the Campaign Coordinator by Maria Page. (In this example. the Digital ID for the attack certificate is 9950 while the one for "real" Paul Butler is 3410.) The message is displayed in red because the Digital ID used for message #4 does not match the original Digital ID that was seen for this email address. This is a spoof message that could easily be sent by an attacker. The Campaign Coordinator should not follow the instructions in Message #4 because it does not come from a trusted source.

Some subjects were confused by this message. One subject didn't understand why the campaign was trying to sign an outside advertising contract to publicize a schedule that is being kept secret. (The subject didn't realize that it's reasonable to purchase outdoor advertising space in advance at locations of planned rallies—both to get the coverage and to prevent the opposing campaign from purchasing the space for attack advertisements.) Another subject didn't understand why there would be a rush to purchase a contract for a campaign rally that was scheduled for many months in the future.

Message #5
From: Sarah Carson <sara_carson_personal@hotmail.com>
To: Campaign Coordinator <ccord@campaign.ex.com>
Subject: Dates for Pennsylvania? Signed: Yes; Digital ID 5999
CoPilot Color: Yellow
Text: Dear Campaign Coordinator,

Hi there! I'm working from home this week and can't access my email from work, so I'm using HotMail.

I'm putting together the art for the Pennsylvania events. I need dates! Can you please send them to my

[1]This message has an extra header, Reply-To: paul_j_butler@hotmail.com, which causes replies to go to the attacker's hotmail account

HotMail account? It's `sara_carson_personal@hotmail.com`.

I'm using HotMail to send this message, so you can probably just hit "reply. "

Thanks so much. I really appreciate this.

—sc

Comment: This is second attack message. In this escalation of the attack, the attacker has created a new HotMail identity that has a name similar to Sarah Carson's (although the Hotmail account is actually misspelled). The message is displayed in yellow because it is the first time that CoPilot has seen a signed email message from this email address; CoPilot has no way of knowing if the Digital ID is legitimate or not because it has never seen the email address sara_carson_personal@hotmail.com before. This message is signed so it carries a digital certificate for sara_carson_hotmail@hotmail.com. Outlook Express sees this certificate and automatically incorporates it into the Campaign Coordinator's address book, making it possible to send a digitally signed, digitally encrypted message to Attacker Sara. Several users fell for this ruse.

Message #6

From: Maria Carson <mpage@campaign.ex.com>
To: Campaign Coordinator <ccord@campaign.ex.com>
Subject: Please send the schedule to Butler and Sarah! Signed: No
CoPilot Color: Gray
Text: Dear Campaign Coordinator,

Hi there! I'm working from home this week and can't access my email from work, so I'm using HotMail.

I'm putting together the art for the Pennsylvania events. I need dates! Can you please send them to my HotMail account? It's `sara_carson_personal@hotmail.com`.

I'm using HotMail to send this message, so you can probably just hit "reply. "

Thanks so much. I really appreciate this.

—sc

Comment: This is the third attack message. In this message, the attacker has forged a message from the mpage email address which tells the Campaign Coordinator to follow the instructions in the previous attack messages. This style of attack, which involves using multiple personae, is in the style of the attacks described in Kevin Mitnick's classic The Art of Deception*[MS02]*.

Message #7

From: Maria Carson <mpage@campaign.ex.com>
To: Campaign Coordinator <ccord@campaign.ex.com>
Subject: Please send the schedule to Ben and Sarah Signed: Yes; Digital ID 3400
CoPilot Color: Green
Text: Dear Campaign Coordinator,

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** (`bend@campaign.ex.com`) and to **Sarah Carson** (`carson@campaign.ex.com`)?

Thanks!

—Maria

Comment: This message is the third legitimate message sent by Maria Carson to the Campaign Coordinator. In it, Carson asks the Coordinator to send the schedule to Sarah Carson, the one Campaign volunteer who has not legitimately received the schedule.

Message #8

From: Maria Carson <mpage@campaign.ex.com>
To: Campaign Coordinator <ccord@campaign.ex.com>
Subject: One last thing... Signed: Yes; Digital ID 3400
CoPilot Color: Green
Text: Dear Campaign Coordinator,

Thanks so much for all of your help today. It's now time for the Debriefing Interview!

—Maria

Comment: This message is the fourth legitimate message sent by Maria Carson to the Campaign Coordinator. It informs the test subject that the test is over.

Discussion
The astute reader may be confused by the fact that the experimental subject was asked to send the same schedule to Ben Donnelly twice—first by Ben, then later by Maria. The explanation is that Maria didn't know that Ben had previously asked for a copy of the schedule, and wants to be sure that he has received it.

C.2.5 Debriefing interview (NoColor)

At the Conclusion of the test, the experimenter turned over the "Initial Task Description" document to reveal the "Debriefing Interview" that was on the other side. Subjects in the **NoColor** group were given the Debriefing Interview shown in Figure C-16, while those in the **Color** and **Color+Briefing** groups were given the Debriefing Interview shown in Figure C-17.

Subjects were permitted to answer the debriefing interview questions in writing or verbally. After the formal questionnaire, the experimenter might ask participants additional questions based aimed at having the subject clarify seemingly contradictory actions. Any questions on the part of the subject were then answered at this time. At this point the recording was stopped, the subject was thanked and paid $20.

Page 2 of 2 Date _____
Subject #: _____ Printed 1/12/2005 2:55 PM

Debriefing Interview:

Interview to follow the CoPilot Usability Test. Please write your answers below or speak them to the experimenter. Thank you!

1. On a scale of 1 to 5, how important did you think the security was in this particular test scenario, where 1 is least important and 5 is most important?

   1 2 3 4 5

2. Do you think that you sent the schedule to someone not associated with the campaign?

   Yes No I don't know

   Comments:

3. Was there anything you thought about doing but then decided not to bother with?

4. Is there anything you think you would have done differently if this had been a real scenario rather than a test?

5. Were there any aspects of the software that you found particularly helpful?

6. Were there any aspects of the software that you found particularly confusing?

7. Are there any other comments you'd like to make at this time?

2

Figure C-16: Debriefing Interview (**NoColor**)

Page 2 of 2 Date _____
Subject #: _____ Printed 1/12/2005 2:56 PM

Debriefing Interview:

Interview to follow the CoPilot Usability Test. Please write your answers below or speak them to the experimenter. Thank you!

1. On a scale of 1 to 5, how important did you think the security was in this particular test scenario, where 1 is least important and 5 is most important?

   1 2 3 4 5

2. Do you think that you sent the schedule to someone not associated with the campaign?

   Yes No I don't know

   Comments:

3. Did you notice the colored borders surrounding the messages?

4. What did the "green" border mean?

5. What did the "red" border mean?

6. What did the "yellow" border mean?

7. What did the "grey" border mean?

8. Was there anything you thought about doing but then decided not to bother with?

9. Is there anything you think you would have done differently if this had been a real scenario rather than a test?

10. Were there any aspects of the software that you found particularly helpful?

11. Were there any aspects of the software that you found particularly confusing?

12. Are there any other comments you'd like to make at this time?

2

Figure C-17: Debriefing Interview (**Color** and **Color+Briefing**)

C.3 Summaries of Test Sessions

C.3.1 Subjects and Ordering

A total of 44 individuals participated in the MIT COUHES-approved protocol between December 21 and January 29. (Eight additional individuals participated in a "pre-test" that took place during the first two weeks of December.)

ID	[2]	Age[3]	Education and Background[4]	Years[5] emailing	Regular email prog[6]	Trial Date	Trial Time
S1	NC	26	pre-PhD, oceanographic engineering	15	Pine	Dec 21	1:00 pm
S2	NC	63	ms, "science"	5	Yahoo	Dec 21	2:57 pm
S3	C	23	B.S. biology/biochem	8	MIT Webmail	Dec 22	3:11 pm
S4	C	23	grad degree, engineering	10	Outlook	Jan 4	11:56 am
S5	C	23	ms student, EECS	9	Evolution	Jan 4	1:00 pm
S6	C	22	some college, business	6	Eudora	Jan 6	3:00 pm
S7	C	44	ms physics, working on CS PhD	10+	Yahoo	Jan 7	8:55 am
S8	NC	58	some college, now an accounting clerk	8	Yahoo	Jan 7	12:10 pm
S9	NC	48	some college, applied math	20	Athena	Jan 7	1:15 pm
S10	C	55	BS, massage therapist	14	Hotmail	Jan 7	2:03 pm
S11	C	28	pre-PhD, in Education	11	Eudora	Jan 7	3:00 pm
S12	C	33	MS, Engineering	10	MIT Webmail	Jan 10	10:20 am
S13	C+B[7]	55	grad degree, arts	5	Webmail	Jan 11	10:00 am
S14	C+B	61	Phd engineering, materials	13	AOL	Jan 11	2:02 pm
S15	NC	37	BS, science writer and editor	9	Eudora	Jan 12	9:40 am
S16	C+B	22	some college, biology	9	MSN Hotmail	Jan 12	4:06 pm
S17	NC	30	MS, mechanical engineering	10	MIT Webmail	Jan 12	5:23 pm
S18	C+B	24	some grad, linguistics and philosophy	11	Outlook Express	Jan 13	12:10 pm
S19	C	30	undergrad, education	8	Outlook	Jan 13	1:42 pm
S20	C+B	19	some college; science and business	10+	MIT Webmail	Jan 14	12:05 pm
S21	NC	23	masters student, ocean engineering	9	Outlook & Webmail	Jan 14	3:30 pm
S22	C+B	52	MBA; does market research	5	Yahoo	Jan 17	2:10 pm
S23	C	21	senior in mathematics	7	Webmail, OE	Jan 19	9:30 am
S24	NC	44	some college; software developer	10	Eudora (PC)	Jan 20	1:11 pm
S25	C	54	masters science writing; science writer	10	Eudora (Mac)	Jan 21	3:15 pm
S26	C+B	43	college; now import/export mgr.	6	Excite Webmail	Jan 21	4:15 pm
S27	C+B	48	master's degree; IS helpdesk	15	pine	Jan 25	9:40 am
S28	C	18	freshman; chemistry	7	Outlook	Jan 25	12:05 pm
S29	NC	60	MA; linguistics, writing	5	AOL & Yahoo	Jan 25	1:30 pm
S30	C+B	46	grad; finance	10	Eudora	Jan 25	3:39 pm
S31	C+B	50	some grad (business); now a paralegal	10	Outlook	Jan 25	5:15 pm
S32	C+B	18	freshman; english	7	webmail & FirstClass	Jan 26	12:59 pm
S33	C	22	some grad; science, astronomy	8	pine & Outlook	Jan 27	1:00 pm
S34	C+B	21	college; finance	10	Outlook & Hotmail	Jan 27	3:00 pm
S35	NC	28	freshman	4	Webmail & Eudora	Jan 27	5:00 pm
S36	C+B	19	senior; engineering	8	Webmail & Evolution	Jan 27	6:30 pm
S37	NC	20	junior; mechanical engineering	7	Webmail	Jan 28	10:45 am
S38	NC	19	sophomore; biology	8	Eudora & webmail	Jan 28	12:18 pm
S39	C+B	35	Phd; physics	7	Yahoo	Jan 28	2:00 pm
S40	NC	22	senior; mechanical engineering	6	MIT Webmail	Jan 28	3:35 pm
S41	C+B	30	grad student; aero astro	9	pine	Jan 28	4:30 pm
S42	C	18	freshman; engineering	8	Eudora; Outlook Express	Jan 29	11:56 am
S43	NC	22	college; computer science	9	gmail; OE	Jan 29	1:06 pm
S44	C+B	20	sophomore; chemistry	8	gmail; First Class	Jan 29	2:18 pm

[2] NC: **NoColor**; C: **Color**; C+B: **Color+Briefing**

[3] intake questionnaire, question 1

[4] intake questionnaire, questions 2, 3

[5] intake questionnaire, question 4

[6] intake questionnaire, question 8

[7] S13 used a preliminary version of the briefing. This user uncovered a variety of problems with the Intervention and, as a result, the decision was made to count this subject as a preliminary or "pre-test" participant. S13's results are not included in our reported statistics.

C.3.2 Key for understanding tables

The following symbology is used in the following sections to discuss the actions and apparent metal states of the experimental subjects:

Symbol	Meaning	Discussion
✓	"Sent"	Subject sent email message as requested.
✗	"Not sent"	Subject made a conscious decision *not* to send the message.
✍	"Signed"	Message was signed with the Subject's key.
✉	"Sealed"	Message was sealed (encrypted) using the actual recipient's key—and not necessarily the intended recipient's key. (PGP makes it possible to seal a message for one recipient and email it to another, but most S/MIME implementations, including Outlook Express, do not have this capability.
👽	"Spoofed"	Subject sent the schedule to one of the Hotmail addresses controlled by the Attacker.
☹?	"Tried"	Subject *tried* to send an encrypted message to Attacker Paul's Hotmail Account, but was stopped by Outlook Express because there was no suitable Digital ID on file for Attacker Paul. These are scored as successful attacks, as the attack would have been successful if Paul had simply attached a digital certificate for his HotMail address to his attack message. The subjects were saved not by their own cleverness, but by the experimenter's oversight.

C.3.3 Results: NoColor

ID	Sec. score	Subject sent schedule when requested by: Maria 1	Maria 2	Ben	Attacker Paul	Attacker Sarah	Attacker Maria	Avoided attacks: any	all	Sent sealed: any	all
S1	4	✓	✓	✓			👽	☺			
S2	5	✓	✓	✓	👽	👽	👽				
S8	5	✓ ✉	✓ ✉	✓ ✉	☹?	👽 ✉ [a]				✉	✉
S9	5	✓ ✍ ✉	✓ ✍ ✉	✓ ✍ ✉	☹?	👽 ✉ [b]	👽 ✉			✉	✉
S15	4	✓ ✍ ✉	✗ [c]	✓ ✍ ✉			👽 ✍ [d]	☺		✉	
S17		✓ ✍	✓ ✍	✓ ✍	👽 ✍	👽 ✍	n/a [e]				
S21	3	✓ ✍ ✉	✓ ✍ ✉	✓ ✍ ✉	☹?	👽 ✍ ✉	👽 ✍			✉	
S24	?	✓ ✍ ✉	✓ ✍ ✉	✓ ✍ ✉	👽 ✍	👽 ✍ ✉	👽 ✍			✉	
S29	5	✓ ✍	[f]	✓ ✍	👽	👽	n/a				
S35	5	✓ ✍	✓ ✍ ✉	✓ ✍		👽 ✍ ✉	👽 [g]	☺		✉	
S37	5	✓	✓ ✍	✓ ✍	👽 ✍	👽 ✍	n/a				
S38	5	✓	✓	✓	👽 ✍		👽 ✍	☺			
S40	4	✓ ✍ ✉	[h]	✓ ✍ ✉	☹?	👽 ✍ ✉		☺		✉	✉
S43	5	✓	✓ ✍ [i]	✓ ✍		👽 [j]	👽 [k]	☺			
14	??	✓ 14/14 ✍ 8 ✉ 6	✓ 11/12 ✍ 7 ✉ 5	✓ 14/14 ✍ 10 ✉ 6	👽 6/14 ✍ 4 ☹? 4/14	👽 11/14 ✍ 6 ✉ 6	👽 9/11 ✍ 4 ✉ 1	☺ 6/14 43%	0%	✉ 7/14 50%	✉ 3/14 21%

[a] Counted as a spoof even though message was not actually sent; S8 would have sent the email to Attacker Sarah, but didn't try because she thought it wouldn't work.

[b] Counted as a spoof, even though the message was not actually sent until after the message from Attacker Maria was received. Like S8, S9 assumed that Hotmail addresses couldn't receive digitally signed e-mail, but unlike S8, S9 sent directions to Attackers Paul and Sarah telling them how to make Digital IDs. When S9 later tried to send Attacker Sarah the digitally signed message, it worked.

[c] S15 wouldn't send the schedule to Ben and Sara's campaign address because she had already sent the schedule to Paul and Sara's Hotmail addresses, at attacker Maria's request, and thought that the legitimate message #7 was in fact an attack message.

[d] S15 apologized for the delay.

[e] There was no need for Attacker Maria to send her message if Attacker Paul and Attacker Sarah were successful in their attacks. The experimenter was inconsistent and sometimes sent the message anyway, however.

[f] S29 didn't read the message and thought that he had already complied

[g] But he couldn't send the message to Attacker Paul because he didn't have a public key for Attacker Paul, and he wanted to send the schedule encrypted.

[h] S40 thought that the emails had already been sent.

[i] S43 forgot to send the message to Sarah.

[j] Sent with the Subject: line "Did you send this?"

[k] Sent with a lecture that Paul and Sarah should "create more obscure account to avoid press leakage, remember: we are in the business of information and secrets!!!

C.3.4 Results: Colors (CoPilot Engaged)

ID	Sec. score	Subject sent schedule when requested by: Maria 1	Maria 2	Ben	Attacker Paul	Attacker Sarah	Attacker Maria	Avoided attacks: any	all	Sent sealed: any	all
S3	5	✓ ✍	✓ ✍	✓ ✍	👽 ✍	👽 ✍	👽 ✍				
S4	4	✓ ✍	✓ ✍	✓ ✍				☺	☺		
S5	4	✓ ✍	✓ ✍	✓ ✍	👽	👽	n/a				
S6	5	✓ ✍ ✉	✓ ✍ ✉	✓ ✍ ✉				☺	☺	✉	✉
S7	4	✓ ✍ ✉	*a*	*b*	☹?		👽 ✍ ✉	☺		✉	✉
S10	5	✓ ✍	✓ ✍	✗	👽 ✍	👽 ✍	👽 ✍				
S11	4	✓ ✍	✓ ✍ *c*	✓ ✍			👽	☺			
S12	5	✗ *d*	✓ ✍	✓ ✍	👽 ✍	👽 ✍	n/a				
S19	5	✓	✓	✓	👽		👽	☺			
S23	5	✓ ✍ ✉	✓ ✍ ✉	*e*				☺	☺	✉	✉
S25	n/a[f]	✓	✓	✓ ✍	👽 ✍	👽 ✍	👽				
S28	5	✓ ✍	✓ ✍	✓ ✍	👽 ✍	👽 ✍	n/a				
S33	1	✓ ✍ ✉	✓ ✍ ✉	✓ ✍ ✉				☺	☺	✉	✉
S42	5	✓ ✍ ✉	✓ ✍ ✉	✓ ✍ ✉	☹?	👽 ✍ ✉	☹?			✉	✉
14	4.4	✓ 13/14 ✍ 11 ✉ 5	✓ 13/13 ✍ 11 ✉ 4	✓ 11/12 ✍ 10 ✉ 3	👽 7/14 ✍ 5 ☹? 2/14	👽 7/14 ✍ 6 ✉ 1	👽 6/12 ✍ 3 ✉ 1 ☹? 1/12	☺ 7/14 50%	☺ 4/14 29%	✉ 5/14 36%	✉ 5/14 36%

[a] S7 sent the schedule signed and encrypted to all campaign members as soon as it was received.

[b] S7 didn't follow Ben's request because the mail had already been sent.

[c] S11 forgot to send the schedule to Sarah Carson

[d] S12 didn't realize Message #2 contained instructions that needed to be acted upon

[e] S23 thought that the message had previously been sent to Ben; in fact, it had been sent to Paul.

[f] S25 refused to provide a rating for security. "I have no idea what the security was. I don't know if it was important or not, because I wasn't aware of any security ever."

C.3.5 Results: Colors + Briefing

ID	Sec. score	Subject sent schedule when requested by: Maria 1	Maria 2	Ben	Attacker Paul	Attacker Sarah	Attacker Maria	Avoided attacks: any	Avoided attacks: all	Sent sealed: any	Sent sealed: all
S14	5	✓ ✍	✓ ✍[a]	✓ ✍				☺	☺		
S16	5	✓ ✍	✓ ✍	✓ ✍				☺	☺		
S18		✓ ✍ ✉	✓ ✍ ✉ [b]	✓ ✍ ✉		👽 ✍ ✉	👽 ✍ ✉ [c]	☺		✉	✉
S20	5	✓ ✍[d]	✓ ✍	n/a[e]	[f]	[g]	👽 ✍[h]	☺			
S22	3	✓ ✍ ✉	✓[i]	✓ ✍ ✉				☺	☺		
S26		✓ ✍	✓ ✍[j]	✓ ✍		👽 ✍		☺			
S27	5	✓ ✍ ✉	✓ ✍ ✉	✓ ✍ ✉		👽 ✍ ✉ [k]	👽 ✍	☺		✉	
S30	5	✗	✗	✓ ✍	👽 [l]	👽	👽				
S31	5	✓ ✍	✓ ✍	✓ ✍	👽 ✍	👽 ✍	n/a				
S32	5	✓ ✍	✓ ✍	✓ ✍		👽 ✍[m]	👽 ✍[n]	☺			
S34	4	✓ ✍	✓ ✍[o]	✓ ✍		👽 ✍	[p]	☺			
S36	4	✓	✓[q]	✓ ✍	[r]	👽 ✍	👽	☺			
S39	5	✗	✓ ✍					☺	☺		
S41	5	✓ ✍ ✉	✓ ✍ ✉	✓ ✍ ✉		👽 ✍ ✉	[s]	☺		✉	✉
S44	5	✓ ✍	✓ ✍	✓ ✍			[t]	☺	☺		
15	??	✓ 13/15 ✍ 12 ✉ 4	✓ 14/15 ✍ 11 ✉ 3	✓ 13/14 ✍ 13 ✉ 4	👽 2/15 ✍ 1	👽 9/15 ✍ 8 ✉ 3	👽 6/14 ✍ 4 ✉ 1	☺ 13/15 87%	☺ 5/15 33%	✉ 3/15 20%	✉ 2/15 13%

[a] S14 inadvertently sent campaign worker Sara Carson's copy of the schedule to attacker Sara Carson's hotmail account due to a usability error in the Outlook Express Interface. Not scored as a spoof in this study because the message was sent in response to campaign worker Maria Page's legitimate email message #7.

[b] Two sets of messages sent: one signed, and one both signed and sealed.

[c] But only sent to Sarah; "I've only sent the message to sarah, for security reasons."

[d] Two copies sent: one not signed, one signed

[e] When he received the schedule from Maria, he immediately sent the schedule to every member of the campaign team.

[f] Sent email to Maria asking for confirmation of new address.

[g] Sent email to Maria asking for confirmation of new address.

[h] Assumed message from Attacker Maria was his confirmation.

[i] Assumed mail already sent to Ben and that "Sara is at home and wants the info via her home hotmail account."

[j] Actually, S26 sent the message to Attacker Sarah because of the OE6 address book usability bug.

[k] Split message into two parts in an attempt to foil any possible attacker.

[l] Copy sent to Ben as well, because he is the IT coordinator and Paul clearly has problems.

[m] Message bounced because Sarah's name was spelled correctly.

[n] With new, correct spelling for Attacker Sarah.

[o] Sent follow-up to Sarah, asking her if she has a HotMail address.

[p] Asked Miria to send the message herself.

[q] Sent to Sarah but not Ben

[r] Asked Paul for his favorite color in an attempt to verify the HotMail persona.

[s] Asked for confirmation with a digitally signed message.

[t] Sent email to Ben asking why Maria was not using her Digital ID

C.4 OpenSSL Configuration

Although there are several commercial and Open Source packages available for creating X.509v(3) certificates, the package of choice appears to be the OpenSSL package. OpenSSL runs on many different computers and has a tremendous cryptographic library, including a full S/MIME imple-

mentation. There are also many tutorials on the Internet that explain how to use OpenSSL to create S/MIME certificates and import those certificates into a variety of applications. One warning sign, however, is that all of these tutorials have different instructions, and many of these instructions are contradictory.

At the root of many of these problems it he fact that OpenSSL was written primarily as a subroutine library. The OpenSSL command-line executable was written as a test bench for this library. it was never designed to be used as a stand-alone application. Thus, the program has poor error handling, poor data handling, and lousy support for interactive use. On the other hand, it is widely used.

OpenSSL Configuration File

OpenSSL requires that a configuration file be present in order for it to be used. This configuration file specifies, among other things, the extensions that OpenSSL will support in the X.509v(3) certificates that it creates and processes. The first complication was that different versions of OpenSSL come with different configuration files, and these different files have different support for extensions. These extensions are, in turn, interpreted differently by different S/MIME clients. The OpenSSL configuration file used to create the certificates used in the *Johnny 2* experiment appear in Section C.4.1 on page 410.

The next step in the process of creating the S/MIME certificates was to decipher the OpenSSL commands for creating a certificate authority. Examples on the Internet invariably include this step, but the certificate authority that they create is not scriptable: there is a passphrase on the CAs private key and most of the creation commands need to be typed interactively.

Creating the CA

It was experimentally determined that a scriptable certification authority could be created satisfactorily with the following commands:

```
% mkdir certs
% echo ``10'' > certs/serial
% cp -f /dev/null certs/index.txt
% openssl req -new -x509 -nodes -keyout certs/cakey.pem \
   -out  certs/cacert.pem -days 1000 \
   -subj '/C=US/ST=California/L=Palo Alto/O=Certification Authority/CN=Certification Manager'
```

Some explanation is in order. The first like creates the `certs` directory which is where the "database" that holds the CA files will be kept. The file `certs/serial` consists of a single line that stores the hexdecimal number of the next certificate that the CA will issue. The file `certs/index.txt` is a text file that contains the serial number and subject of *every* certificate that the CA has allegedly created. (Or, at least, those that have been recorded.)

Now we are ready to consider the options for the OpenSSL command:

req	The CA request system should be employed. This has the effect of creating a private key and a corresponding public key.
-new	A new certificate should be created.
-x509	Make an x509 self-signed certificate rather than a certificate signing request.
-nodes	"No DES." That is, do not use DES (or any other symmetric encryption algorithm) to encrypt the certificate's private key. It is a common mistake to read this argument as the plural of the word "node." It is important that the CA private key be stored without encryption—otherwise, the experimenter would have been forever typing and retyping passphrases while trying to get everything set up.
-keyout certs/cakey.pem	Place the private key in the specified file.
-out certs/cacert.pem	Place the public key in the file certs/cacert.pem.
-days 1000	Make the certificate good for a little less than 3 years.
-subj '...'	Specifies the subject that will be present on the X509 certificate. Notice that this field is itself divided into subfields for city, state, locale, organization, and Common Name.

Creating each persona certificate
Each persona certificate is created with more-or-less the same set of commands. Here are the commands for for creating the Campaign Coordinator's public/private keypairs and OpenSSL certificate:

```
% echo "7283" > certs/serial
% CAMPAIGN=/C=US/ST=Pennsylvania/L=Philadelphia/O=Campaign Coordination
% openssl req -config openssl.cnf -new -nodes \
  -subj '\$(CAMPAIGN)/CN=Campaign Coordinator/emailAddress=ccord@campaign.ex.com' \
  -keyout certs/ccord.key -out certs/ccord.csr
% openssl ca -batch -config openssl.cnf  -in certs/ccord.csr  -out certs/ccord.crt
```

The `openssl req` command in this example is much the same as the req command that was used to create the CA key, with two exceptions, both having to do with certificate's subject field. First, because this certificate will be used for S/MIME, it has the "emailAddress=" subfield as specified by PKCS #9 and referenced in RFC 3850.[Ram04a] Second, because the "emailAddress=" field makes this command far, far too long for one line, the common fields for campaign workers have been placed in the environment variable CAMPAGIN. Because the "-x509" switch is not present, the "req" subcommand creates a certificate signing request (CSR), rather than a self-signed request.

Once the CSR has been created, it is necessary to sign the certificate. This operation is performed by the OpenSSL "ca" command. The meanings of the options specified are reasonably clear and need not be explained.

As it turns out, Windows cannot import an x509 private/public key pair unless the two are combined in a PKCS12 file. This combination can be done using the following command:

```
% openssl pkcs12 -export -passout pass:"" -in certs/ccord.crt \
  -inkey certs/ccord.key -out certs/ccord.pfx -name 'Campaign Coordinator'
```

The "-passout" command specifies the password that is used to encrypt the private key. OpenSSL supports numerous password encryption schemes; in this case, the "pass:" character string specifies that the rest of the argument will specify a password as a plaintext character string. We specify no password because passwords are a drag to type when setting up certificates for fictional personas.

Importing the *Johnny 2* S/MIME Certificates Windows and OE6
Once certificates were created, they needed to be imported into Windows and OE6. Importing the certificates was imported because the Campaign Coordinator is informed "Digital IDs for Paul, Ben, Sarah and Dana have been pre-loaded onto your machine by the IT Coordinator." One advantage of importing these certificates is that it allowed the Campaign Coordinator to send encrypted email messages to each of the campaign participants without having to first obtain their public key certificates. Instead of relying on importation, the scenario could have relied on CoPilot's support for third-party certificates, since the first message from Maria Page is cc'ed to the other campaign members and therefore includes third-party certificates for those individuals.

Here once again, the proper way to do this under Windows was not immediately clear. We were pleased to discover that the Campaign Coordinator's certificate could be imported by double-clicking on the PKCS12 file and adding it to the appropriate Windows certificate store with the Certificate Import Wizard.(check name). Attempts to import the other certificates in this way proved fruitless, however.

After much experimentation, it was determined that the easiest way to import third-party S/MIME certificates into Outlook Express was to email Outlook Express S/MIME messages that were signed with the certificates that we desired to import. This created both the OE6 address book entry and imports the certificate into the Windows certificate store. (Double-clicking on the certificate and importing it with the appropriate Windows wizard imports the certificate to the certificate store, but did not create the necessary Outlook Express address book entry.) For each certificate this generated an Outlook warning because the CA key that was used to sign these certificates was not explicitly trusted.[8] We were able to edit the trust parameters for each S/MIME certificate and cause Outlook Express to explicitly trust that certificate in particular. In this manner, we were able to get OE6 to simulate the Key Continuity manner—at least to the point that OE6 would not warn us when it saw these certificates. Once again, if CoPilot were fully operational, these manual "Wizard of Oz" steps would have been performed automatically by the software.

[8]Well, we didn't want to trust the CA—it's private key was compromised because it wasn't stored encrypted on the hard drive!

C.4.1 OpenSSL configuration file

This section includes the relevant statements (but not the comments) of the Johnny 2 OpenSSL configuration file

```
HOME = .
RANDFILE = $ENV::HOME/.rnd
oid_section = new_oids

[ new_oids ]

[ ca ]
default_ca = CA_default # The default ca section

[ CA_default ]

dir = certs/ # Where everything is kept
certs = $dir/certs # Where the issued certs are kept
crl_dir = $dir/crl # Where the issued crl are kept
database = $dir/index.txt # database index file.
new_certs_dir = $dir # default place for new certs.

certificate = $dir/cacert.pem  # The CA certificate
serial = $dir/serial  # The current serial number
crl = $dir/crl.pem  # The current CRL
private_key = $dir/cakey.pem # The private key
RANDFILE = $dir/.rand # private random number file

x509_extensions = usr_cert # The extentions to add to the cert

name_opt  = ca_default # Subject Name options
cert_opt  = ca_default # Certificate field options

default_days = 365 # how long to certify for
default_crl_days= 30 # how long before next CRL
default_md = md5 # which md to use.
preserve = no # keep passed DN ordering
policy = policy_match

# For the CA policy
[ policy_match ]
countryName = match
stateOrProvinceName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
emailAddress = optional

[ policy_anything ]
countryName = optional
stateOrProvinceName = optional
localityName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
```

```
emailAddress = optional

[ req ]
default_bits = 1024
default_keyfile  = privkey.pem
distinguished_name = req_distinguished_name
attributes = req_attributes
x509_extensions = v3_ca # The extentions to add to the self signed cert
string_mask = nombstr

[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = US
countryName_min = 2
countryName_max = 2
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Pennsylvania
localityName = Locality Name (eg, city)
localityName_default = Philadelphia

0.organizationName = Organization Name (eg, company)
0.organizationName_default = Campaign Coordination

organizationalUnitName = Organizational Unit Name (eg, section)
organizationalUnitName_default = Certification Authority

commonName = Common Name (eg, YOUR name)
commonName_max = 64
emailAddress = Email Address
emailAddress_max = 64


[ req_attributes ]
challengePassword = A challenge password
challengePassword_min = 0
challengePassword_max = 20

unstructuredName = An optional company name
[ usr_cert ]

basicConstraints        = CA:FALSE
nsCertType              = client, email, objsign
keyUsage                = nonRepudiation, digitalSignature, keyEncipherment
nsComment = "OpenSSL Generated Certificate"

subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid,issuer:always
subjectAltName          = email:copy

[ v3_req ]
basicConstraints       = CA:FALSE
keyUsage               = nonRepudiation, digitalSignature, keyEncipherment

[ v3_ca ]
subjectKeyIdentifier   = hash
```

```
authorityKeyIdentifier = keyid:always,issuer:always
basicConstraints       = critical,CA:true
keyUsage               = cRLSign, keyCertSign
nsCertType             = sslCA, emailCA
subjectAltName         = email:copy
issuerAltName          = issuer:copy

[ crl_ext ]
authorityKeyIdentifier=keyid:always,issuer:always

[ smime_all ]
nsCertType = email
keyUsage = critical,digitalSignature,keyEncipherment
extendedKeyUsage = emailProtection
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
subjectAltName = email:move

[ smime_sign ]
nsCertType = email
keyUsage = critical,digitalSignature
extendedKeyUsage = emailProtection
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
subjectAltName = email:move

[ smime_encrypt ]
nsCertType = email
keyUsage = critical,keyEncipherment
extendedKeyUsage = emailProtection
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
subjectAltName = email:move
```