Aligning Security and Usability with Key Continuity Management



Simson L. Garfinkel Harvard Center for Research on Computation and Society http://www.simson.net/

I've been doing Security & Usability.

There seem to be two main ways that this work has proceeded:

- X Work on authentication (hard problem).
- ✗ Work on new interfaces.
- × Work on underlying rules and principles.

I'm taking a different track for aligning security and usability:

- Re-evaluating underlying models and mechanisms so that we can get more security with our existing interfaces.
 - File Sanitization
 - Secure Messaging
- Finding the best ideas and trying to put them all in one place.
- Working with vendors like Microsoft and Apple to incorporate these ideas into their products.

First project: Hard drive deletion

I purchased 250+ hard drives on the secondary market between 1998 and 2002.

- Many of the disks contained confidential information [Garfinkel & Shelat, IEEE S&P '03]
- Most of the confidential information could only be recovered using forensic tools.
- Hypothesis: people had been trying to erase the info, but their tools were not very good.



The trace-back study revealed that many cases involved the failure of a trusted organization or individual to correctly sanitize the drive before disposing of it.

Second Project: Email security survey

- Survey of 470 Amazon.com merchants in US and UK.
- 20% had been receiving S/MIME-signed messages for a year.
- Majority (72%) thought that receipts sent *from merchants* should be digitally signed, sealed with encryption or both
- Garfinkel et. al, FC2005 and CHI2005

Third Project: Enabling Email security through opportunistic encryption and Key Continuity Management

- Stream an opportunistic PGP proxy
- CoPilot a design of Stream for S/MIME
- Johnny 2 a user test of CoPilot

This presentation focuses on the use and promise of Key Continuity Management

1. Why KCM can help solve the secure messaging problem

2. CoPilot: Implementing KCM with S/MIME and Outlook Express

3. Johnny 2: A user test of KCM





PHONE

Secure Messaging — email that is *signed* and *sealed* — seems to be the grand challenge of usability and security.

- Public key cryptography was developed for secure messaging.
- This project is nearly thirty years old:
 - → 1976 Diffie Helman
 - → 1977 RSA
 - → 1987 RFC 989 (PEM)
 - → 1991 PGP Released
 - → 1996 S/MIME
- Today we use public key cryptography for SSH, SSL, and code signing but there's virtually no secure email.

Either it's really hard to get this right, or nobody really cares.

People do care about email security. (Garfinkel et al, FC05)

In our study of Amazon.com merchants:

- 59% thought that email receipts from online merchants should be digitally signed.
- 47% thought receipts should be sealed

And they have the tools — sort of.

- 45% respondents would upgrade their email client to get more security.
- 54% of those using S/MIME-capable mail clients didn't know that they could receive digitally signed mail!

We should also want email security, because security could help with the largest security threats we face today:

- Phishing
- Spam

These threats can be addressed with signing alone.

So why is nobody sending signed mail? Why don't *businesses* like VeriSign send signed mail???

Gutmann argues that the emphasis on certification has been a distraction. [Gutmann 05]

STARTTLS in SMTP, POP and IMAP has secured far more email than S/MIME or PGP.

Most of these certificates appear to be self-signed.

heck with your system administrator before changing any of he advanced options below:						
Automatically synchronize changed mailboxes						
IMAP Path Prefix:						
Port:	143	🗹 Use SSL				
Authentication:	Password					

Perhaps the problem is that the CA approach is fundamentally not very usable.

Recall that a certificate is a statement signed by a CA that binds a key to a particular Common Name (CN):



The theory is that humans understand names, not public keys.

Ellison argues that certified names are useless because names are not unique, not even within a company. [Ellison 02]



Certification has proven to be the hard problem that is gating secure email.

An alternative is to directly certify relationships:



We rarely want to send confidential information on the first try. We first verify that the person can receive it, that they are reading their mail, etc.

PGP avoided this problem

Phil Zimmerman handed me PGP 2.0 on a floppy with his key.

At that same party, somebody else gave me their key's fingerprint on a business card.



Today if you want to email somebody, you get their PGP key off their web page — or ask them to email you their PGP key.

The Stream SMTP and POP transparent proxy was a kind of automatic PGP assistant. [Garfinkel DGo'03]

Stream:

- Made PGP keys on the fly when it detected new From: address;
- ✓ Hid user's PGP key in the outgoing email header.
- Automatically incorporated keys that were discovered.

Planned but never implemented:

- → Alert user if a correspondent's key changes.
- → Automatically distribute and back up private keys.

The real problem with Stream was that PGP has poor penetration and poor usability.

Most of Stream's goals can be achieved with S/MIME, by changing the certification model.

- S/MIME distributes certificates by sending them with signed mail.
- You need a transparent, zero-click way to make new certificates:
 - Option 1: create self-signed certificates.
 - Option 2: Some sort of automatic email answer-back system.
- You need an expert that watches the certificates used for signing and alerts on new (cert, addr) combinations.

CoPilot Implements the Key Continuation Management interface on top of Outlook Express.

	t View Tools Mess	age Help		~		<i></i>
Sech:	Bachi All Forward	Drint Dalata	Breakour	V	0ddaaraar	
From: Date: To: Ec: Subject: Security:	Maria Page Tuesday, February 08, ccord@campaign.ex.co Paul Butler; Ben Donnel Welcome to the Campai Digitally signed and veri	2005 11:18 AM m ly; Sarah Carson; Dana gn! fied	McIntyre			8
						^
From:	Maria Page <	mpage@campai	gn.ex.com	-		
Subje	ct: Welcome to th	ie Campaign!				
To:	ccord@camp	aign.ex.com				
Cc:	Paul Butler <b <bend@camp <carson@can <dmi@campa< td=""><th>utler@campaign paign.ex.com>, S npaign.ex.com>, aign.ex.com></th><th>.ex.com>, E arah Carso Dana McIn</th><td>Ben Do on tyre</td><td>nnelly</td><td></td></dmi@campa<></carson@can </bend@camp </b 	utler@campaign paign.ex.com>, S npaign.ex.com>, aign.ex.com>	.ex.com>, E arah Carso Dana McIn	Ben Do on tyre	nnelly	
	This message is have received for The message w	s yellow because it rom this email add as signed using Dig	is the first si ress. gital ID #3400	gned m).	essage that you	,
		e .				

New Key



Same Key

Reply Reply All Forward Print Delete Previous Next Addresses	~
m Paul Buller Het Skurdøy, January 29, 2005 2:37 PM corofilkompagin, e.c.com Sject: Something is wrong with my email comtifie til something is wrong with my email comtifie til something is something and and writed	8
	^
From: Paul Butler <butler@campaign.ex.com></butler@campaign.ex.com>	
Subject: Something is wrong with my email!	
To: ccord@campaign.ex.com	=
This message is red because email from Paul Butter different Digital #3410. This message was sent using Digital ID #9960.	(ID
Dear Campaign Coordinator,	VOU

Changed key



No Key



.

Normal Communications



New Key Attack: (Forged From:, New Cert)



New Identity Attack (From Hotmail, New Cert)



Unsigned Message Attack (Forged From:, No Cert)



Can untrained end-users resist these attacks?

The original plan: Test KCM with Whitten's "Why Johnny Can't Encrypt" protocol.

- Scenario: A campaign volunteer sending out the schedule to other campaign workers.
- Whitten's test subjects rapidly suspended their disbelief.
- Use Johnny as our control group: see if KCM has a higher success rate and lower spoof rate than PGP.

Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0 Alma Whitten School of Computer Science Carnegie Mellon University Pittsburgh, PA 15213 alma@cs.cmu.edu J. D. Tygar¹ EECS and SIMS University of California Berkeley, CA 94720 tygar@cs.berkeley.edu Abstract 1 Introduction User errors cause or contribute to most computer Security mechanisms are only effective when used security failures, yet user interfaces for security still correctly. Strong cryptography, provably correct tend to be clumsy, confusing, or near-nonexistent. Is protocols, and bug-free code will not provide security if this simply due to a failure to apply standard user the people who use the software forget to click on the interface design techniques to security? We argue that, encrypt button when they need privacy, give up on a on the contrary, effective security requires a different communication protocol because they are too confused usability standard, and that it will not be achieved about which cryptographic keys they need to use, or through the user interface design techniques appropriate accidentally configure their access control mechanisms to other types of consumer software. to make their private data world-readable. Problems To test this hypothesis, we performed a case study such as these are already quite serious: at least one of a security program which does have a good user researcher [2] has claimed that configuration errors are interface by general standards: PGP 5.0. Our case the probable cause of more than 90% of all computer study used a cognitive walkthrough analysis together security failures. Since average citizens are now with a laboratory user test to evaluate whether PGP 5.0 increasingly encouraged to make use of networked can be successfully used by cryptography novices to computers for private transactions, the need to make achieve effective electronic mail security. The analysis security manageable for even untrained users has found a number of user interface design flaws that may become critical [4, 9]. contribute to security failures, and the user test This is inescapably a user interface design demonstrated that when our test participants were given problem. Legal remedies, increased automation, and 90 minutes in which to sign and encrypt a message user training provide only limited solutions. Individual using PGP 5.0, the majority of them were unable to do users may not have the resources to pursue an attacker so successfully. legally, and may not even realize that an attack took We conclude that PGP 5.0 is not usable enough to place. Automation may work for securing a provide effective security for most computer users, communications channel but not for setting access despite its attractive graphical user interface, supporting control policy when a user wants to share some files our hypothesis that user interface design for effective and not others. Employees can be required to attend security remains an open problem. We close with a training sessions, but home computer users cannot. brief description of our continuing work on the Why, then, is there such a lack of good user development and application of user interface design interface design for security? Are existing general user principles and techniques for security interface design principles adequate for security? To answer these questions, we must first understand what kind of usability security requires in order to be 1 Also at Computer Science Department, Carnegie Mellon University (on leave).

The idea of comparing results directly with *Johnny* didn't quite work out.

- Johnny didn't have an attacker
- Johnny didn't use third-party certification
 it used email answerback certification.

(Therefore, Johnny only protected against a passive attacker.)

- Whitten said that the results were qualitative.
- Details of the original protocol had been lost.

The Johnny 2 Scenario:

It's Whitten's Scenario, except:

- The subject plays the role of a campaign volunteer.
- Three developed personas:
 - Maria The Campaign Manager.
 - Sarah Graphic artist.
 - **Paul** Campaign treasurer
 - **Ben** IT Coordinator.
- The enemy campaign tries to steal documents through a spoofing attack.
- The attacker pretends to be Paul, Sarah, and Maria in a series of escalating attacks.

Big Question to answer:

What will the users do when faced with the attacks?

New Key Attack	Attacker Paul says that he is having computer problems (new key, old email address).
New Identity Attack	Attacker Sarah says she is working from home and using Hotmail.
Unsigned Message Attack	Attacker Maria sends mail from her Campaign account, but it's not signed.

Other questions that the *Johnny 2* scenario can answer:

- Do users understand the difference between signing and sealing?
- If users can trivially sign/seal their email, will they?
- If users can seal confidential information before they send it, will they be less concerned about the destination?

The big question we don't need to answer:

Is it just as secure as CA model?

This isn't a fair question...

... KCM doesn't replace the CA, it replaces no crypto at all!

... If you have a CA, you can still use the CA model.

Johnny 2 User Study

Recruiting posters at MIT.

43 subjects aged 18–63 ($\bar{x} = 33, \sigma = 14.2$)

19 Men, 24 Women

17 to 57 minutes $(\bar{t} = 41, \sigma = 10.32)$

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 <u>simsong@mit.edu</u>

0 Security Study mson 7-876-6111 nsong@mit.edu	0 Security Study mson 7-876-6111 nsong@mit.edu nson 0 Security Study mson mson mson mson	0 Security Study mson 7-876-6111 msong@mit.edu	0 Security Study mson 7-876-6111 msong@mit.edu	0 Security Study mson 7-876-6111 msong@mit.edu	0 Security Study mson 7-876-6111 msong@mit.edu
\$20 Sims 517- sims	\$20 \$17- \$20 \$20 \$17- \$17- \$20	\$20 Sims sims	\$20 Sims 517- sims	\$20 Sims 517-	\$20 Sims 517- sims

Three Cohorts compared. No Color



Color



Color + Briefing



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

Scenario Message 1: Greetings from Maria Page

🔿 Welc	A Welcome to the Campaign!						
File	Edit View Tools Message Help						
&							
Reply Reply All Forward Print Delete Previous Next Addresses From: Maria Page Image Imag							
Security: Digitally signed and verified From: Maria Page <mpage@campaign.ex.com> Subject: Welcome to the Campaign! To: ccord@campaign.ex.com Paul Butler <butler@campaign.ex.com>, Ben Donnelly <bend@campaign.ex.com>, Sarah Carson <carson@campaign.ex.com>, Dana McIntyre <dmi@campaign.ex.com> This message is yellow because it is the first signed message that you have received from this email address. The message was signed using Digital ID #3400.</dmi@campaign.ex.com></carson@campaign.ex.com></bend@campaign.ex.com></butler@campaign.ex.com></mpage@campaign.ex.com>							
De	Dear Campaion Coordinator.						

Orients user and provides list of campaign worker roles.

Scenario Message 2: Maria sends the schedule

2) Speakir	ng dates f	for Pennsy	/lvania					
	File Edi	t View	Tools Me:	ssage Help					_
	€≁		48		×		0	W	
1	Reply	Reply All	Forward	Print	Delete	Previous	Next	Addresses	_
From: Maria Page Date: Tuesday, January 18, 2005 10:49 PM To: ccord@campaign.ex.com Subject: Speaking dates for Pennsylvania Security: Digitally signed and verified									
Γ									^
	From	Mari	a Page -	<mpage@< th=""><td>) campai</td><td>gn.ex.con</td><td>n></td><td></td><th></th></mpage@<>) campai	gn.ex.con	n>		
	Subje	ct: Spe	aking da	tes for Pe	nnsylvan	ia			
	To: ccord@campaign.ex.com								
		This	s messag	ge is gree	n becau	se you			
		hav	e receive	ed 2 mess	sages fro	m this	stop ti	rusting this ID	
		Digi	ital ID (#	3400)					
	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								
	is av	ailable a	at all time	98.	ui ne où	10 17/01 01	iodal on		····

Tests to see if the subject can follow directions.

Scenario Message 3: Ben asks for the schedule

🖴 I need a copy of the Pennsylvania dates!						
File Edit View Tools Message Help	1					
Set Set Name Reply Reply All Forward Print Delete Previous Next Addresses						
From: Ben Donnelly Date: Saturday, January 29, 2005 2:36 PM To: ccord@campaign.ex.com Subject: I need a copy of the Pennsylvania dates! Security: Digitally signed and verified						
From: Ben Donnelly <bend@campaign.ex.com> Subject: I need a copy of the Pennsylvania dates! To: ccord@campaign.ex.com This message is green because the sender's Digital ID was already installed on the computer. This is the first message that you have received from this Digital ID (#4159)</bend@campaign.ex.com>						
Dear Campaign Coordinator,	~					

Will the subject trust a legitimately signed message?

Scenario Message 4: Attacker Paul asks for schedule

Something is wrong with my email!	
File Edit View Tools Message Help	
See See Next Next Reply Reply All Forward Print Delete Previous Next Addresses	
From:Paul ButlerDate:Saturday, January 29, 2005 2:37 PMTo:ccord@campaign.ex.comSubject:Something is wrong with my email!Security:Digitally signed and verified	8
From: Paul Butler <butler@campaign.ex.com> Subject: Something is wrong with my email! To: ccord@campaign.ex.com This message is red because email from Paul Butler <butler@campaign.ex.com> was previously sent using different Digital #3410. This message was sent using Digital ID #9950.</butler@campaign.ex.com></butler@campaign.ex.com>	
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?	~

New Key Attack (combined with a Reply-To: attack)

Scenario Message 5: Attacker Sarah asks for schedule

🖴 Dates for Pennsylvania?						
File Edit View Tools Message Help						
Image: Second						
From:Sarah CarsonDate:Saturday, January 29, 2005 2:41 PMTo:ccord@campaign.ex.comSubject:Dates for Pennsylvania?Security:Digitally signed and verified	8					
From: Sarah Carson <sara_carson_personal@hotmail.com> Subject: Dates for Pennsylvania? To: ccord@campaign.ex.com This message is yellow because it is the first signed message that you have received from this email address. The message was signed using Digital ID #5999.</sara_carson_personal@hotmail.com>						
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	~					

New identity attack

Scenario Message 6:

Attacker Maria demands that schedule be sent to attackers Paul and Sarah

🖴 Please send the schedule to Butler and Sarah!					
File Edit View Tools Message Help	7				
Reply Reply All Forward Print Delete Previous Next Addresses					
From:Maria PageDate:Saturday, January 29, 2005 2:43 PMTo:ccord@campaign.ex.comSubject:Please send the schedule to Butler and Sarah!					
	^				
From: Maria Page <mpage@campaign.ex.com></mpage@campaign.ex.com>					
Subject: Please send the schedule to Butler and Sarah!					
To: ccord@campaign.ex.com					
This message is gray because it was not sent using a Digital ID and the sender of this message usually uses Digital IDs					
Dear Campaign Coordinator,					
I can't call you. Something is wrong with the phones in the office. I've tried calling you twice and I keep getting a fast busy. I just got off the phone with Paul and Sara and they both are having the same problem.					
Diese cend a controf the Condidate's schedule immodiately to both Paul Rutler	~				

Unsigned message attack

Scenario Message 7:

Maria Page asks that schedule be sent to Sarah and Ben

🚔 Please send the schedule to Ben and Sarah						
File Edit View Tools Message Help						
See See Next See Reply Reply All Forward Print Delete Previous Next Addresses						
From:Maria PageDate:Saturday, January 29, 2005 2:49 PMTo:ccord@campaign.ex.comSubject:Please send the schedule to Ben and SarahSecurity:Digitally signed and verified	8					
	^					
From: Maria Page <mpage@campaign.ex.com> Subject: Please send the schedule to Ben and Sarah To: ccord@campaign.ex.com This message is green because you have received 3 messages from this Digital ID (#3400)</mpage@campaign.ex.com>]					
Dear Campaign Coordinator,						
Hi once again! We're going to be wrapping things up here pretty soon. You've been really great so far.	~					

Another test or "control" message

Scenario Message 8: Maria Page thanks the subject

🚔 One last thing				
File Edit View Tools Message Help	a 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 1997 - 199			
Seply Reply All Forward Print D	Previous Next Addresses			
From:Maria PageDate:Tuesday, February 08, 2005 11:20 AMTo:ccord@campaign.ex.comSubject:One last thingSecurity:Digitally signed and verified	A			
From: Maria Page <mpage@ca< td=""> Subject: One last thing To: ccord@campaign.ex.com This message is green to have received 4 message Digital ID (#3400)</mpage@ca<>	aign.ex.com> use you rom this stop trusting this ID			
Dear Campaign Coordinator,				
Thanks so much for all of your help Interview!	ay. It's now time for the Debriefing			

This proved to be a nice way to end the experiment.

Results, Task Comprehension:

Most subjects:

- Understood and enjoyed the scenario.
- Understood the concept of a "signed message" as authenticating the sender.
- Didn't realize that signing prevented message modification

Many people who were attacked didn't realize it at all; some realized it after-the-fact.

Many users struggled to authenticate the new identity and unsigned messages.

- A few people looked at the digital signature using Microsoft's certificate tools. They saw that the message was signed, but didn't know what it meant.
- Many users tried Email answer-back. A few mistook Attacker Maria's message for an answer to a message that was sent.
- Roughly half the users asked for the phone.

Well, we didn't let them use the phone



"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."

KCM was very successful against the New Key Attack:

No Color











A Red Border ... someone else is trying to impersonate the sender.



KCM works well against the Unsigned Message Attack:

No Color











A Gray Border ... someone else who is trying to impersonate the sender.



KCM didn't help against the New Identity Attack:

No Color











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



The New Identity Attack is successful because the indicators are ambiguous!

- The attack matches a common situation in real-life.
- Subjects said that they knew there was a risk, but decided to ignore it.
- Only two noticed that Sarah's name was misspelled!

Evaluating the Usability of Encryption:

- Suprisingly, more people in NoColor encrypted than in Color or Color+Briefing
- It appears that they were (incorrectly) using encryption as a proxy for authentication
- Many people were confused by the Sign and Encrypt buttons in the OE interface

		Clicked "encrypt"	
		to seal email	
Colort	n	sometimes	always 🛛
NoColor	14	50%	21%
Color	14	36%	36%
Color+Briefing	15	20%	13%
p =		0.087	0.59



Interesting failings:

- Subjects were confused regarding single-click vs. double-click. They would double-click the "encrypt" button to no result!
- Subjects wanted to know how to make a Digital ID for Attacker Paul so they could send him the schedule!

Evaluation of CoPilot's Interface:

- People liked the colors, didn't read the text, and didn't understand the button
- People ignored the headers
- Serious confusion on commands vs. status on buttons
- Heavy users of web mail were the most confused.



Conclusion and Recommendations:

- We've previously argued that much commercial mail sent by eBay, Amazon, etc., should be signed.
- Johnny 2 shows that people can understand and use KCM with little or no training.
- S/MIME is much more usable than people give it credit.
- The hard thing is getting a certificate.
- KCM gives people certificates automatically, but leaves them susceptible to the New Identity Attack. (This is the phishing problem.)

Deployment Strategies:

- You could build this in right now.
- Or Microsoft & Thawte could work together to make it easier for people to get email-only certificates.

We can improve usability and security by making better use of the tools we have already deployed.

Merchants like Amazon, eBay and PayPal should use S/MIME to sign their outgoing mail.

Most of what key continuity management offers can be accomplished with e-mail only S/MIME certificates.

A "CoPilot" that explains what certificates means can increase understanding, which increases usability and security.



Acknowledgements: Rob Miller, David Clark

Questions?