Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten and J.D. Tygar

Usenix Sec'99



ABOUT PROGRAMS COURSES PEOPLE RESEARCH CAREERS

Why Johnny Can't Encrypt: Doug Tygar's Landmark Paper Stands the Test of Time

Admin

- Reading Report
- TA email: security101_ta@syssec.kaist.ac.kr

User Interface Failures

Humans

"Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic o perations. (They are also large, expensive to maintain, difficult to manage, an d they pollute the environment. It is astonishing that these devices continue t o be manufactured and deployed. But they are sufficiently pervasive that we must design our protocols around their limitations.)"

> - C. Kaufman, R. Perlman, and M. Speciner. Network Security: PRIVATE Communication in a PUBLIC World. 2nd edition. Prentice Hall, page 237, 2002.

Humans are weakest link

- Most security breaches attributed to "human error"
- Social engineering attacks proliferate
- Frequent security policy compliance failures
- Automated systems are generally more predictable and accurate than humans

Why are humans in the loop at all?

- Don't know how or too expensive to automate
- Human judgments or policy decisions needed
- Need to authenticate humans

The human threat

- Malicious humans who will attack system
- Humans who are unmotivated to perform securitycritical tasks properly or comply with policies
- Humans who don't know when or how to perform secur ity-critical tasks
- Humans who are incapable of performing securitycritical tasks

Need to better understand humans in the loop

- Do they know they are supposed to be doing something?
- Do they understand what they are supposed to do?
- Do they know how to do it?
- Are they motivated to do it?
- Are they capable of doing it?
- Will they actually do it?

Internet Security Warning

Sleep warning

prevented this.



The server you are connected to is using a s that cannot be verified.

Your laptop will not sleep if you shut the lid as a running program has

Some laptops can overheat if they

not sleep when the lid is closed.

👩 Allow access

X

Allow application access to keyring?

The application 'evolution-alarm-notify' (/usr/lib/evolution/2.22/ evolution-alarm-notify) wants to access the password for 'Google://http://www.google.com/calendar/feeds/ cristian.bravo@gmail.com/private/full' in the default keyring.



×

Are you sure you want to turn on private browsing?

When private browsing is turned on, webpages are not added to the history, items are automatically removed from the Downloads window, information isn't saved for AutoFill (including names and passwords), and searches are not added to the popup menu in the Google search box. Until you close

Encryption Problems

Microsoft Office Outlook had problems encrypting this message because the following recipients had missing or invalid certificates, or conflicting or unsupported encryption capabilities:

mitsu@intermail.co.il

Continue will encrypt and send the message but the listed recip may not be able to read it.

Send Unencrypted

Continue

Security Warning

"C:\Documents and Settings\user name\Local Settings\Temporary Internet Files\test.doc" contains macros.

Macros may contain viruses. It is usually safe to disable macros, but if the macros are legitimate, you may lose some functionality.



SSL Warnings



High Risk of Security Compromise

Your connection to *cameo.library.cmu.edu* is either being intercepted by another party or someone is impersonating *cameo.library.cmu.edu*.

An attacker is attempting to steal information that you are sending to *cameo.library.cmu.edu*. We advise you to contact this company by telephone or using a different computer that does not yield this warning.

Get Me Out of Here!

Why was this site blocked?

Ignore this warning

False Alarm Effect

- "Detection system" ≈ "System"
- If risk is not immediate, warning the user will decrease

OK



her

Are you sure you want to turn on private browsing?

When private browsing is turned on, webpages are not added to the history, items are automatically removed from the Downloads window, information isn't saved for AutoFill (including names and passwords), and searches are not added to the popup menu in the Google search box. Until you close the window, you can still click the Back and Forward buttons to return to webpages you have opened.



Phishing

Spear Phishing (Targeted Phishing)

Personalized mail for a (small) group of targeted users
 Employees, Facebook friends, Alumni, eCommerce Customers
 These groups can be obtained through identity theft!

□ Content of the email is personalized.

Different from Viagra phishing/spam

- □ Combined with other attacks
 - Zero-day vulnerability: unpatched
 - ▶ Rootkit: Below OS kernel, impossible to detect with AV software
 - ▶ Key logger: Further obtain ID/password
 - ► APT (Advanced Persistent Threat): long-term surveillance

Examples of Spear Phishing

Soundby	rteF10 D X Inbox X	Print all	Expand all	Forwar	rd al
👌 from	Michael Jordan cs_umn_news@yahoo.com	hid	e details Feb 21	Reply	V
to	hopper@cs.umn.edu				
date	Mon, Feb 21, 2011 at 6:11 AM				
subject	SoundbyteF10				
mailed-by	cs.umn.edu				
signed-by	yahoo.com				
External 4-192 K 200 Uni Minnear Phone: (nd Events Contacts Relations Coordinator eller Hall on Street SE polis, MN 55455 612) 625-2424				
Email: <u>n</u>	ews@cs.umn.edu (External Relations Coordinator)				

Good Phishing example



world of warcraft: Cataclysm Beta Test Invitation!

Get those opt-ins ready for the World of Warcraft: Cataclysm closed beta! The sundering of Azeroth is nigh, and you don't want to be left out in the cold of Northrend when you could be enjoying the sun-drenched beaches on the goblin isle of Kezan. To ensure you're opted-in and eligible as a potential candidate, you'll need a World of Warcraft license attached to your Battle.net account, have your current system specifications uploaded to the Battle.net Beta Profile Settings page, and have expressed interest through the franchise-specific check boxes.

Get the Installer - Log in to your Battle.net account :

CONCERNMENT OF THE OF THE OWNER OWNER OF THE OWNER OWNER

Enjoy the game!

Alma Whitten



Why Johnny can't encrypt?

• PGP 5.0

- Pretty Good Privacy
- Software for encrypting and signing data
- Plug-in provides "easy" use with email clients
- Modern GUI, well designed by most standards
- Usability Evaluation following their definition

If an average user of email feels the need for privacy and authentication, and acquires PGP with that purpose in mind, will PGP's current design allow that person to realize what needs to be done, figure out how to do it, and avoid dangerous errors, without becoming so frustrated that he or she decides to give up on using PGP after all?

Defining Usable Security Software

- Security software is usable if the people who are expected to use it:
 - are reliably made aware of the security tasks they need to perform.
 - are able to figure out how to successfully perform those tasks
 - don't make dangerous errors
 - are sufficiently comfortable with the interface to continue using it.

Why is usable security hard?

- The unmotivated users
 - "Security is usually a secondary goal"
- Policy Abstraction
 - Programmers understand the representation but normal users have no background knowledge.
- The lack of feedback
 - We can't predict every situation.
- The proverbial "barn door"
 - Need to focus on error prevention.
- The weakest link
 - Attacker only needs to find one vulnerability

Usability Evaluation Methods

- Cognitive walk through
 - Mentally step through the software as if we were a new user. Attempt to identify the usability pitfalls.
 - Focus on interface learnablity.

Deculto		PGPtools 🛛 🗉 🗄						1	Dra	ag users from this list to the Recipients list:	Yalidity Trust		Size		
Resi	Results								0	Michael lannamico <mji@pgp.com></mji@pgp.com>			1024/4021	^	
										0	Noah Dibner Salzman <noah@cytochrome.com></noah@cytochrome.com>			1024/2048	
						常				0	Noah Dibner Salzman <noah@pgp.com></noah@pgp.com>			1024/2048	
										0	PGP Support Key DSS <pgpsupport@pgp.com></pgpsupport@pgp.com>			1024/1024	
			PGPkeys	Encrypt	Sign Encr	ypt & S	Sign D	ecrypt/Verify		0	Philip Nathan <philipn@pgp.com></philipn@pgp.com>			1024/2048	
		l	1							0	Philip R. Zimmermann <prz@pgp.com></prz@pgp.com>			1024/2048	
		GPkey	<i>c</i>		-					0				1024/2048	
		Эгкеу	5							0	Will Price <wprice@pgp.com></wprice@pgp.com>			1024/4000	
		Name			Yalidity		Creation	Size		0	Will Price <wprice@primenet.com></wprice@primenet.com>			1024/4000	
	▽	🕮 Alma Whitten <	alm. Postomutedu)	>			9/24/98	1024/2048							•
										_					_
			ten <alma@cs.cmu< th=""><th>.edu></th><th></th><th></th><th></th><th></th><th></th><th>-</th><th></th><th></th><th></th><th>.</th><th></th></alma@cs.cmu<>	.edu>						-				.	
	`	_	ten <alma@cs.cmu whitten <alma@cs.< th=""><th></th><th></th><th></th><th>9/24/98</th><th></th><th></th><th>Rec</th><th>cipients :</th><th>¥alidity</th><th>Trust</th><th>Size</th><th>_</th></alma@cs.<></alma@cs.cmu 				9/24/98			Rec	cipients :	¥alidity	Trust	Size	_
		_	whitten <alma@cs.< th=""><th></th><th></th><th></th><th>9/24/98 5/14/97</th><th>1024/4096</th><th></th><th>Rec</th><th></th><th>Yalidity</th><th>Trust</th><th>Size</th><th></th></alma@cs.<>				9/24/98 5/14/97	1024/4096		Rec		Yalidity	Trust	Size	
	•	🗨 Alma V	whitten <alma@cs. b@pgp.com></alma@cs. 	.cmu.edu>				1024/4096 1024/2048			- Jason Bobier <jbobier@prismatix.com></jbobier@prismatix.com>	Validity	Trust		
		Alma \ Bill Blanke <wjt< th=""><th>whitten <alma@cs. b@pgp.com> is <bat@pgp.com></bat@pgp.com></alma@cs. </th><th>.cmu.edu></th><th></th><th></th><th>5/14/97</th><th></th><th></th><th>ß</th><th>- Jason Bobier <jbobier@prismatix.com></jbobier@prismatix.com></th><th>¥alidity</th><th>Trust</th><th>1024/2059</th><th><u></u></th></wjt<>	whitten <alma@cs. b@pgp.com> is <bat@pgp.com></bat@pgp.com></alma@cs. 	.cmu.edu>			5/14/97			ß	- Jason Bobier <jbobier@prismatix.com></jbobier@prismatix.com>	¥alidity	Trust	1024/2059	<u></u>
		Alma \ @== Bill Blanke <wjt @== Brett A. Thoma</wjt 	whitten <alma@cs. b@pgp.com> is <bat@pgp.com> jason@pgp.com></bat@pgp.com></alma@cs. 	.cmu.edu>			5/14/97 5/19/97	1024/2048		ß	- Jason Bobier <jbobier@prismatix.com></jbobier@prismatix.com>	Validity	Trust	1024/2059	-
		Alma \ D== Bill Blanke <wjt D== Brett A. Thoma D== Jason Bobier <j< th=""><th>whitten <alma@cs. b@pgp.com> is <bat@pgp.com> jason@pgp.com> eff@pgp.com></bat@pgp.com></alma@cs. </th><th>.cmu.edu></th><th></th><th></th><th>5/14/97 5/19/97 6/4/97</th><th>1024/2048</th><th></th><th>ß</th><th>- Jason Bobier <jbobier@prismatix.com></jbobier@prismatix.com></th><th>Validity</th><th>Trust</th><th>1024/2059</th><th>-</th></j<></wjt 	whitten <alma@cs. b@pgp.com> is <bat@pgp.com> jason@pgp.com> eff@pgp.com></bat@pgp.com></alma@cs. 	.cmu.edu>			5/14/97 5/19/97 6/4/97	1024/2048		ß	- Jason Bobier <jbobier@prismatix.com></jbobier@prismatix.com>	Validity	Trust	1024/2059	-
	A A A A A	Alma A Dee Bill Blanke (wjl Dee Brett A. Thoma Dee Jason Bobier (j Dee Jeff Harrell (je	whitten <alma@cs. b@pgp.com> is <bat@pgp.com> jason@pgp.com> eff@pgp.com> ller <jis@mit.edu></jis@mit.edu></bat@pgp.com></alma@cs. 	.cmu.edu>			5/14/97 5/19/97 6/4/97 5/20/97	1024/2048 1024/2059 1024/2048		ß	- Jason Bobier <jbobier@prismatix.com></jbobier@prismatix.com>	¥alidity	Trust	1024/2059	•
	A A A A A A A	Alma A Des Bill Blanke (wjl Des Brett A. Thoma Des Jason Bobier (j Des Jeff Harrell (je Des Jeffrey I. Schill	whitten <alma@cs. b@pgp.com> is <bat@pgp.com> jason@pgp.com> eff@pgp.com> ller <jis@mit.edu> ude@pgp.com></jis@mit.edu></bat@pgp.com></alma@cs. 	.cmu.edu>			5/14/97 5/19/97 6/4/97 5/20/97 8/27/94	1024/2048 1024/2059 1024/2048 1024		ľ	- Jason Bobier <jbobier@prismatix.com> Philip R. Zimmermann <prz@acm.org></prz@acm.org></jbobier@prismatix.com>	Validity	Trust	1024/2059	*
	A A A A A A A A A	Alma A Dee Bill Blanke (wjl Dee Brett A. Thoma Dee Jason Bobier (j Dee Jeff Harrell (je Dem Jeffrey I. Schill De jude shabry (ju	whitten <alma@cs. b@pgp.com> is <bat@pgp.com> jason@pgp.com> eff@pgp.com> iller <jis@mit.edu> ude@pgp.com> ers <1loyd@pgp.co</jis@mit.edu></bat@pgp.com></alma@cs. 	.cmu.edu>			5/14/97 5/19/97 6/4/97 5/20/97 8/27/94 6/9/97	1024/2048 1024/2059 1024/2048 1024 1024 1024/2048			Jason Bobier <jbobier@prismatix.com> Philip R. Zimmermann <prz@acm.org></prz@acm.org></jbobier@prismatix.com>	Yalidity		1024/2059	
		Alma A Dee Bill Blanke «wil Dee Brett A. Thoma Dee Jason Bobier <j Dee Jeff Harrell <je Dem Jeffrey I. Schil Dee jude shabry <ju Dee Lloyd L. Chamber</ju </je </j 	whitten <alma@cs. b@pgp.com> is <bat@pgp.com> jason@pgp.com> eff@pgp.com> iler <jis@mit.edu> ide@pgp.com> ers <1loyd@pgp.con></jis@mit.edu></bat@pgp.com></alma@cs. 	.cmu.edu>			5/14/97 5/19/97 6/4/97 5/20/97 8/27/94 6/9/97 5/20/97	1024/2048 1024/2059 1024/2048 1024 1024/2048 1024/2048 1024/4096			- Jason Bobier <jbobier@prismatix.com> Philip R. Zimmermann <prz@acm.org></prz@acm.org></jbobier@prismatix.com>	Yalidity	Trust	1024/2059	-

Cognitive Walk Through Results

- Irreversible actions
 - Need to prevent costly errors
- Consistency
 - Status message: "Encoding"?!?
- Too much information
 - More unneeded confusion
 - Show the basic information, make more advanced information available only when needed.

1	Fil	e Edit	Keys Help									
			Sign	ж s				VI NUYS				_
			Add Name Set Default	жD	PGPkeys			- Name	Yalidity	Trust	Creation	Size
Ē	B			₩N			\neg	🞏 Alma Whitten <alm th="" වංදනයාගය්ථ<=""><th></th><th></th><th>9/24/98</th><th>1024/204</th></alm>			9/24/98	1024/204
- 1	P	GPI	New Key Info	ж∎ Ж∣			\neg	🕃 Alma Whitten <alma@cs.cmu.edu></alma@cs.cmu.edu>				
- 1		Name	Keyserver		Get Selected Key	жG		🍓 Alma Whitten <alma@cs.cmu.edu></alma@cs.cmu.edu>			9/24/98	
- 1	$\overline{}$	蹄 Alma		жR	Send Selected Key			III Blanke <wjb@pgp.com></wjb@pgp.com>			5/14/97	1024/409
- 1	\neg	3 A	Revoke		Find New Keys	ЖF		🕮 Brett A. Thomas (hat@non.com)			5/19/97	1024/204
		n ©≊ Bill B	Export Keys.		·du>							

User Test

- User Test
 - PGP 5.0 with Eudora
 - 12 participants all with at least some college and none with advanced knowledge of encryption
 - Participants were given a scenario with tasks to complete within 90 min
 - Tasks built on each other
 - Participants could ask some questions through email

User Test Results

- 3 users accidentally sent the message in clear text
- 7 users used their public key to encrypt and only 2 of the 7 figured out how to correct the problem
- Only 2 users were able to decrypt without problems
- Only 1 user figured out how to deal with RSA keys correctly.
- A total of 3 users were able to successfully complete the basic process of sending and receiving encrypted emails.
- One user was not able to encrypt at all

Conclusion

• Reminder

If an average user of email feels the need for privacy and authentication, and acquires PGP with that purpose in mind, will PGP's current design allow that person to realize what needs to be done, figure out how to do it, and avoid dangerous errors, without becoming so frustrated that he or she decides to give up on using PGP after all?

• Is this a failure in the design of the PGP 5.0 interface or is it a function of the problem of traditional usable design vs. design for usable secure systems?

Discussion

- Usable security is not constrained in software
 - Generally, embedded device's usability is not good
 - Low quality display -> Not good feedback
 - Analog interface -> Complex
 - -> Usable security is more insufficient!
 - Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System





Web Browser Security User Interfaces

Internet Explorer 9

http://www.google.com/	*	Ç	>
M https://mail.google.com/mail/?shva=1#inbox	23	Ç	>
🗢 https://www.bankofamerica.com/p 🔎 👻 🔒 Bank of America Corporati	2	Ç	>

Firefox 4

http://www.google.com/	☆▼	C
google.com https://mail.google.com/mail/?shva=1#inbox	☆▼	C
Bank of America Corporation (US) https://www.bankofamerica.com	☆▼	C

Chrome 8

🔇 www.google.com

https://mail.google.com/mail/?shva=1#inbox

Bank of America Corporation [US] https://www.bankofamerica.com/privacy

Safari 4

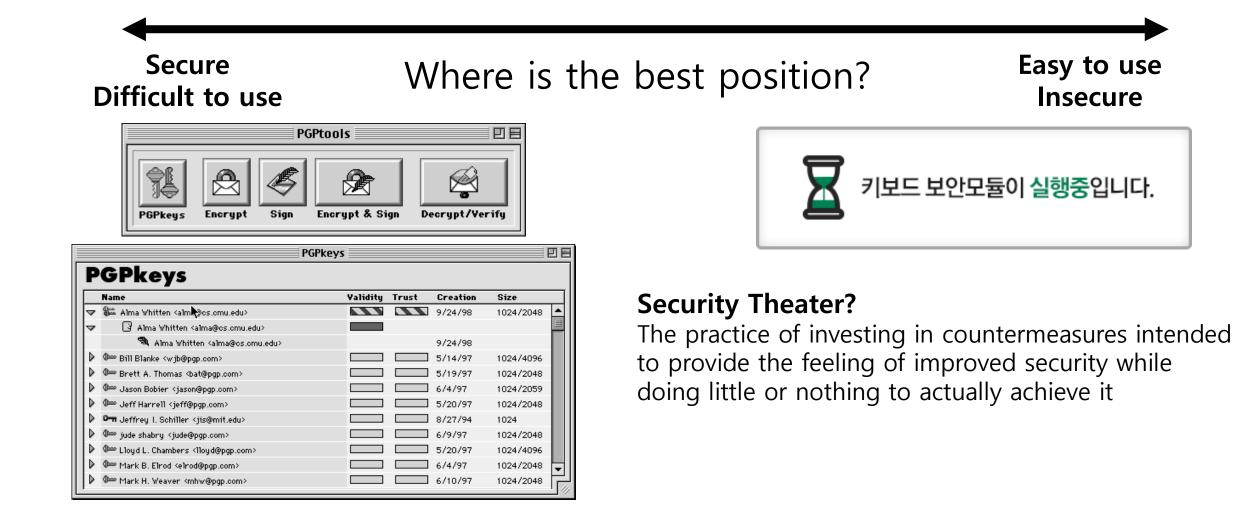


Firefox 3.6 M google.com https://www.google.com/accounts/ServiceLogin?se $rac{1}{2}$ bottom-right corner of browser window (status bar): Firefox 3.0 M https://www.google.com/accounts/ServiceLogin?service=mail&rac{1}{2} bottom-right corner of browser window: www.google.com Firefox 2.0 M https://www.google.com/accounts/ServiceLogin?service=mail&rac{1}{2} bottom-right corner of browser window: www.google.com Firefox 2.0

bottom-right corner of browser window: www.google.com 🔗

Why these browsers have made changes?

Tradeoff between usability and security



Conclusion

- Design user interface considering usable security
- Select a proper security protocol depending on application
 - Financial apps need high-level security