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

Alma Whitten and J.D. Tygar

Usenix Sec'99

Aug 18, 2015

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?

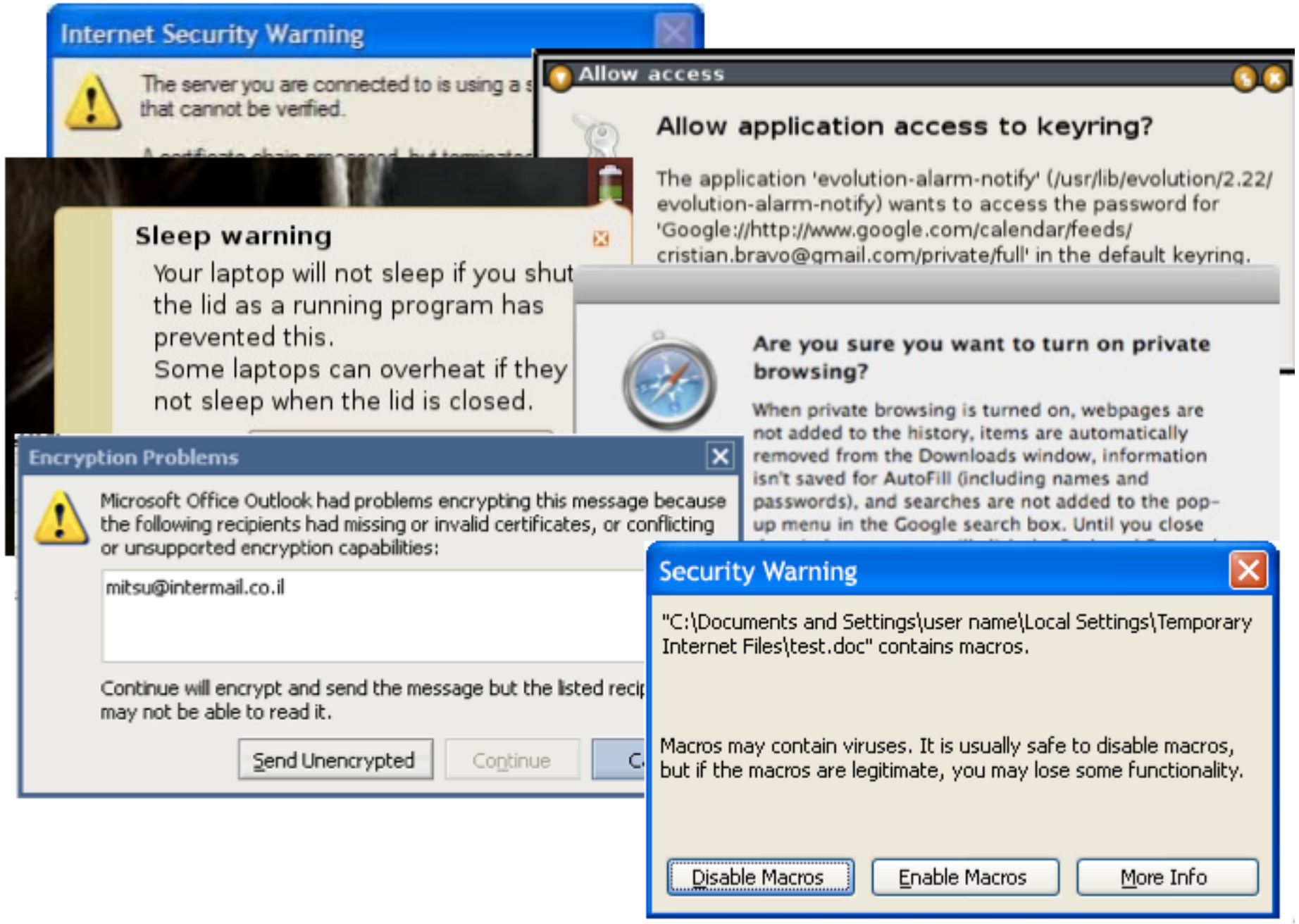
- Don’t know how or too expensive to automate
- Human judgments or policy decisions needed
- Need to authenticate humans

The human threat

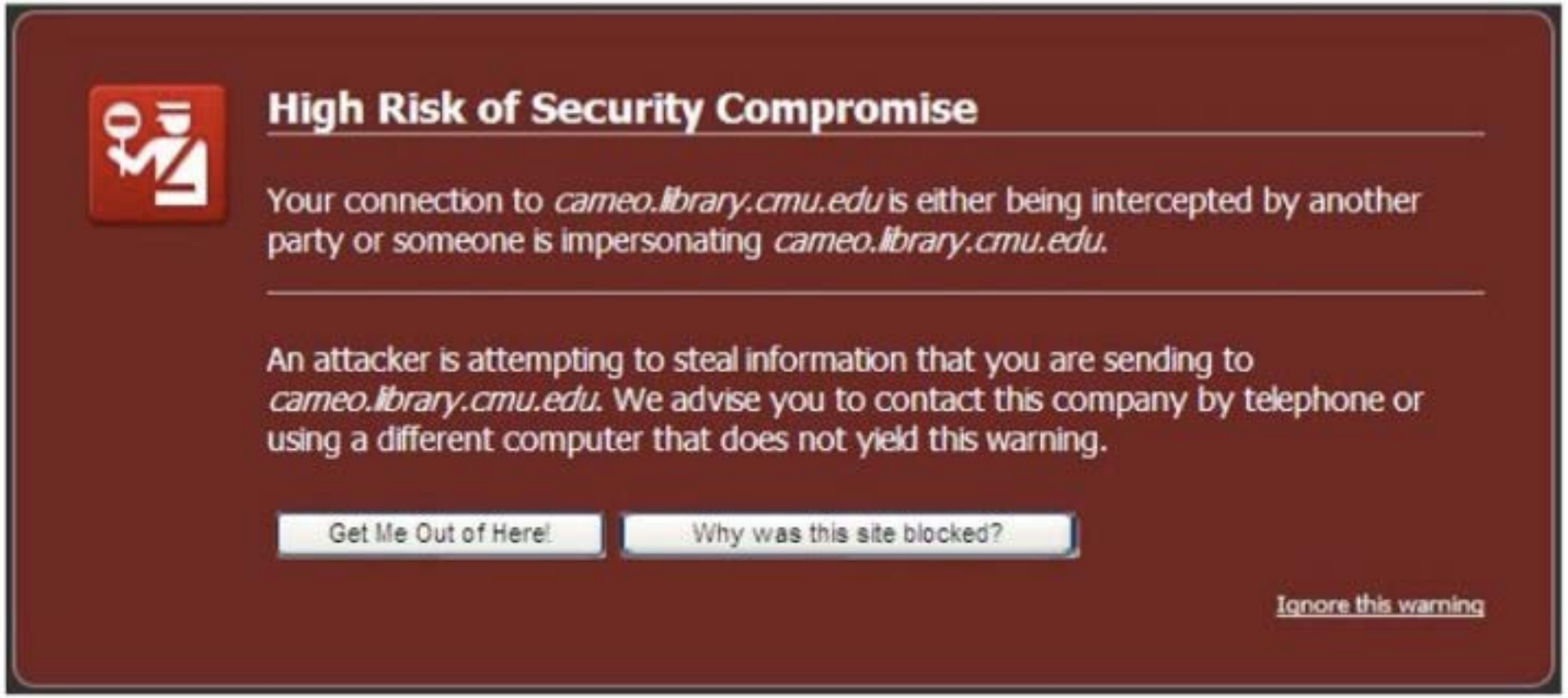
- Malicious humans who will attack system
- Humans who are unmotivated to perform security-critical tasks properly or comply with policies
- Humans who don’t know when or how to perform secur ity-critical tasks
- Humans who are incapable of performing security-critical tasks

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
The server you are connected to is using a s
that cannot be verified.
Allow access
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.
Sleep warning
Your laptop will not sleep if you shut
the lid as a running program has
prevented this.
Some laptops can overheat if they
not sleep when the lid is closed.
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 pop-up 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.
Disable Macros
Enable Macros
More Info

SSL Warnings



False Alarm Effect

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

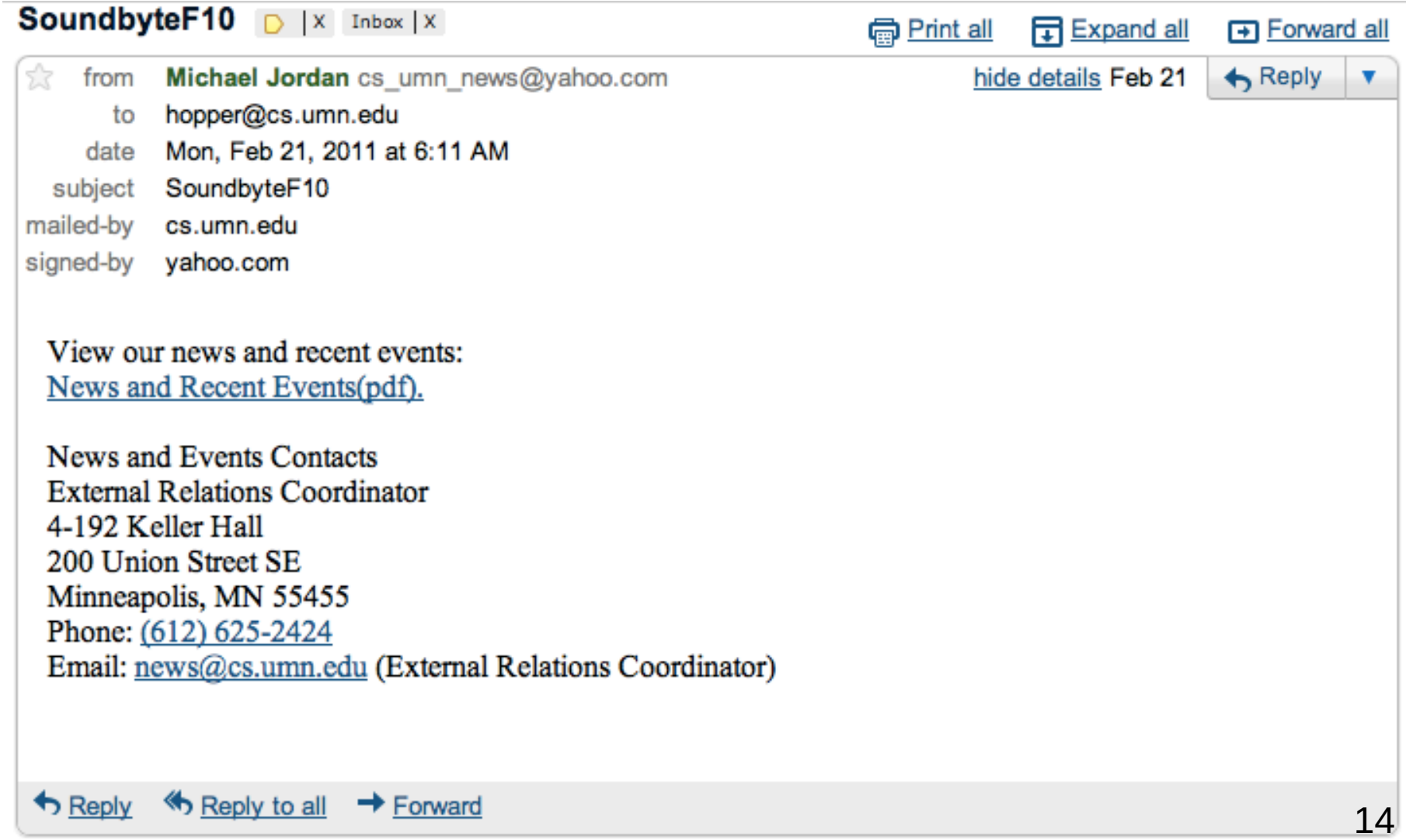
Phishing

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



SoundbyteF10 | X Inbox | X

Print all Expand all Forward all

from **Michael Jordan** cs_umn_news@yahoo.com hide details Feb 21 Reply

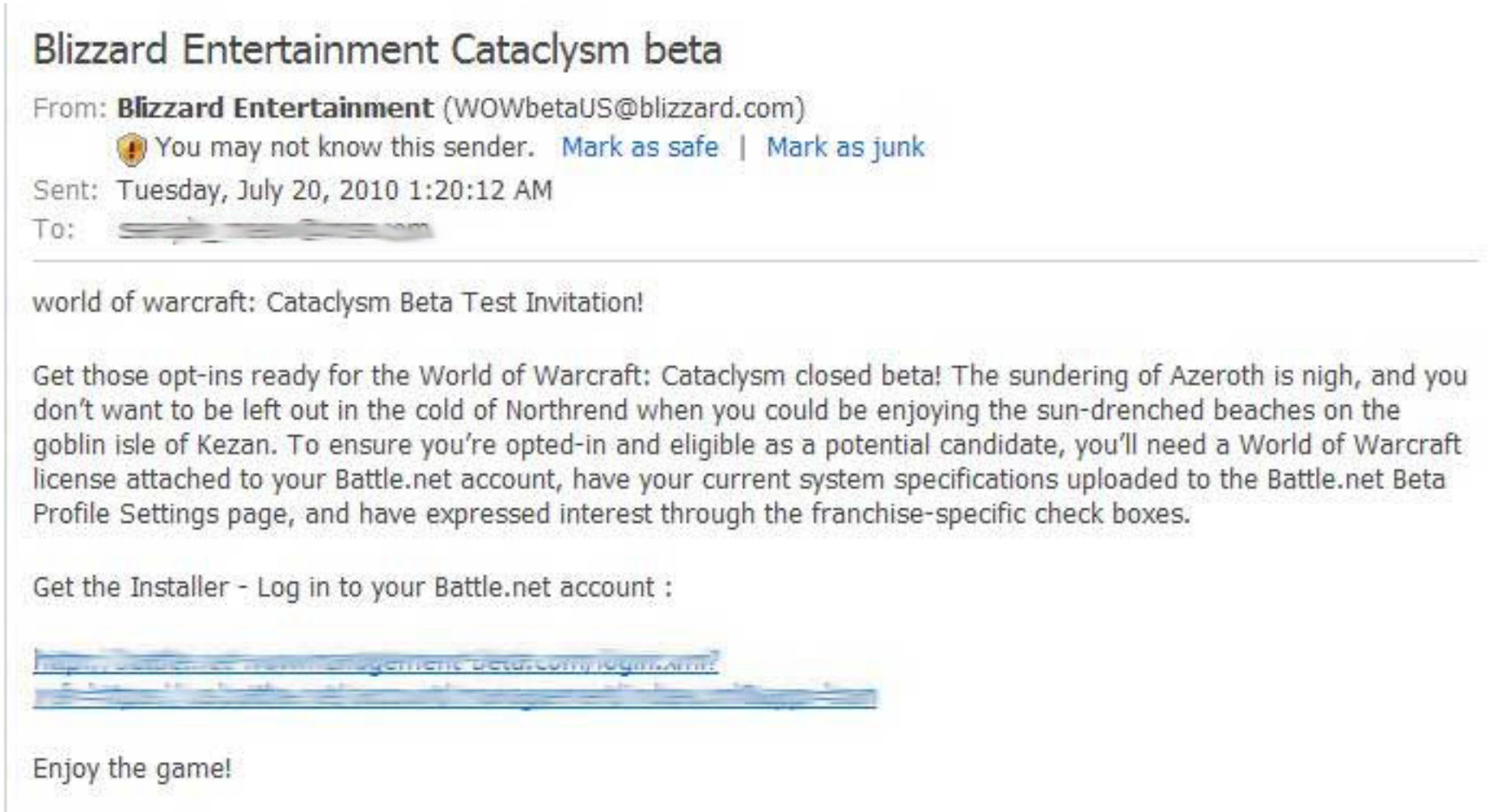
to hopper@cs.umn.edu
date Mon, Feb 21, 2011 at 6:11 AM
subject SoundbyteF10
mailed-by cs.umn.edu
signed-by yahoo.com

View our news and recent events:
News and Recent Events(pdf).

News and Events Contacts
External Relations Coordinator
4-192 Keller Hall
200 Union Street SE
Minneapolis, MN 55455
Phone: (612) 625-2424
Email: news@cs.umn.edu (External Relations Coordinator)

Reply Reply to all Forward

Good Phishing example



Blizzard Entertainment Cataclysm beta

From: **Blizzard Entertainment** (WOWbetaUS@blizzard.com)

You may not know this sender. Mark as safe | Mark as junk

Sent: Tuesday, July 20, 2010 1:20:12 AM

To: [redacted]

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 :

[redacted]

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

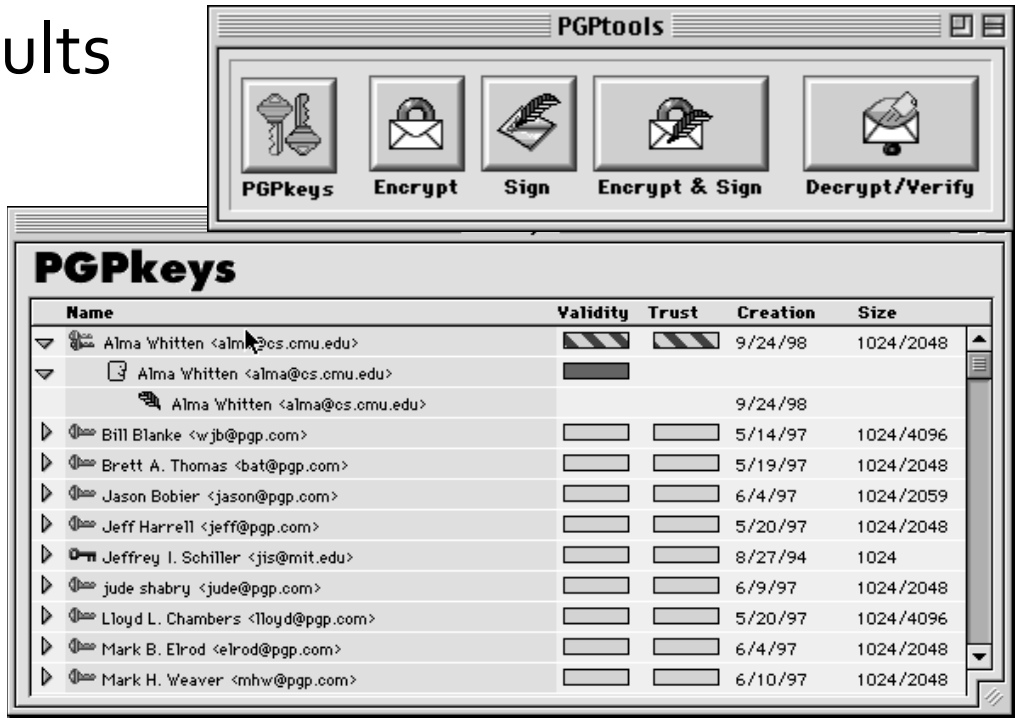
- Security software is usable if the people who are expected to use it:
  - are reliably made aware of the security tasks they need to perform.
  - are able to figure out how to successfully perform those tasks
  - don't make dangerous errors
  - are sufficiently comfortable with the interface to continue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

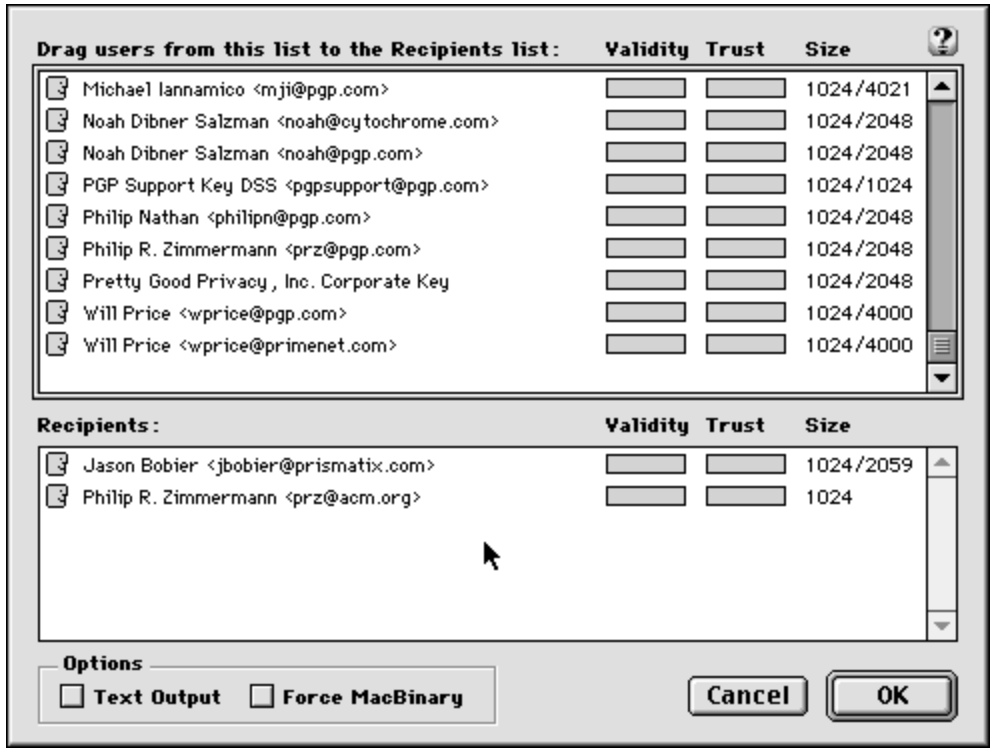
Why is usable security hard?

- 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

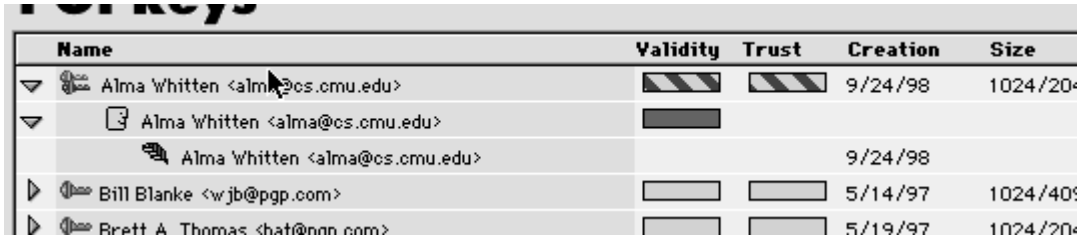
- Cognitive walk through
  - Mentally step through the software as if we were a new user. Attempt to identify the usability pitfalls.
  - Focus on interface learnablity.
- Results





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.



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

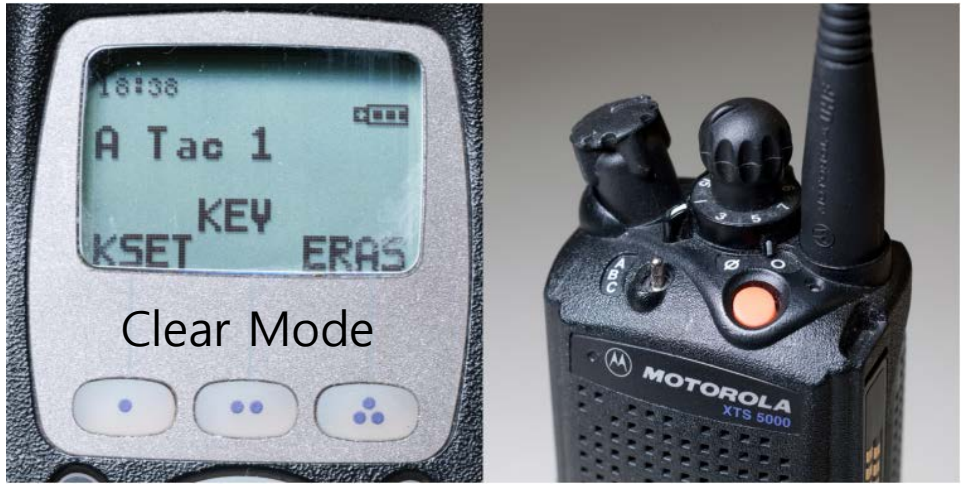
  > If an average user of email feels the need for privacy and authentication, and acquires PGP with that purpose in mind, will PGP's current design allow that person to realize what needs to be done, figure out how to do it, and avoid dangerous errors, without becoming so frustrated that he or she decides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

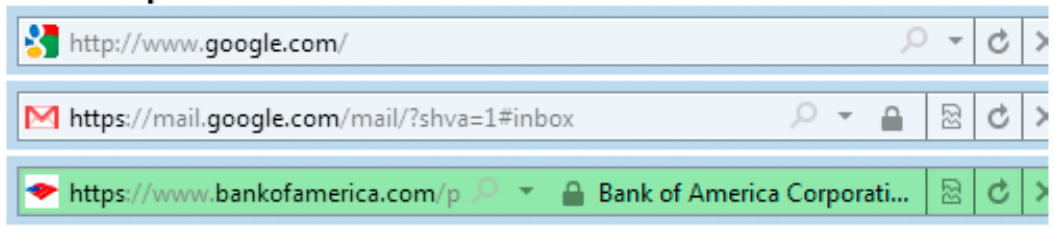


Clear Mode

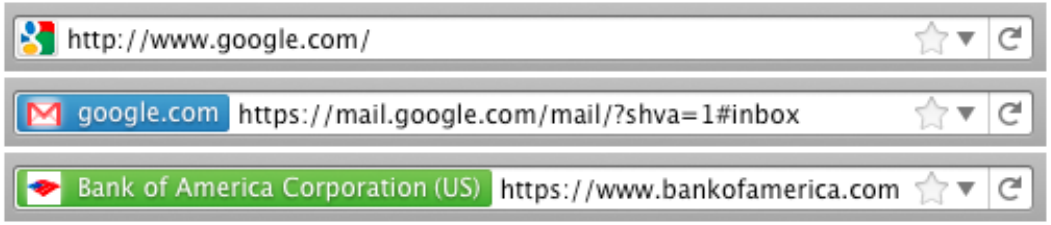
Encrypted Mode

Web Browser Security User Interfaces

Internet Explorer 9

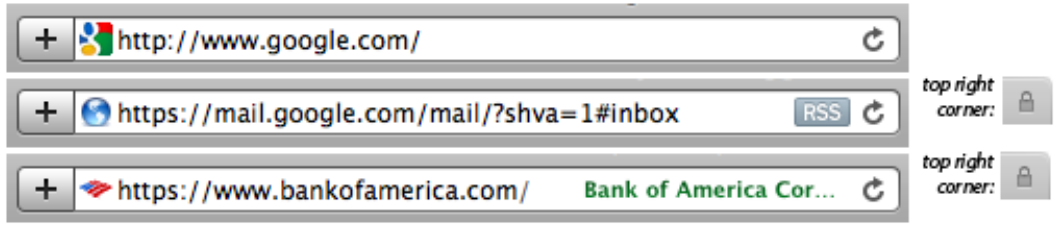


Firefox 4



Chrome 8

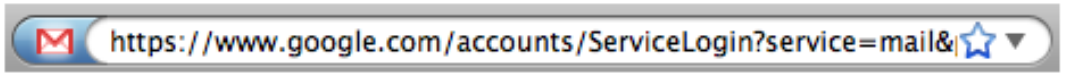
Safari 4



Firefox 3.6

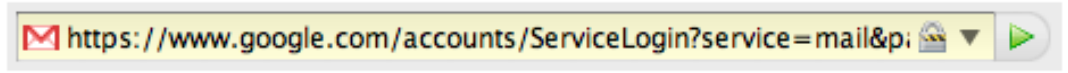
bottom-right corner of browser window (status bar):

Firefox 3.0



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

Firefox 2.0



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

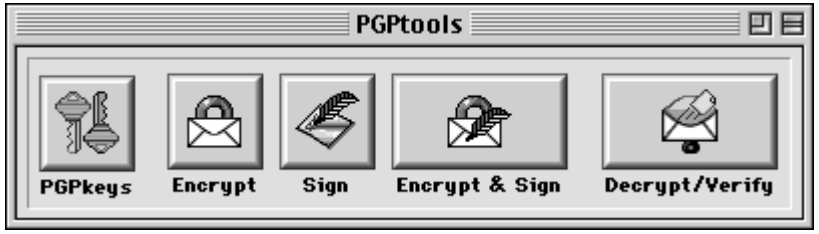
Why these browsers have made changes?

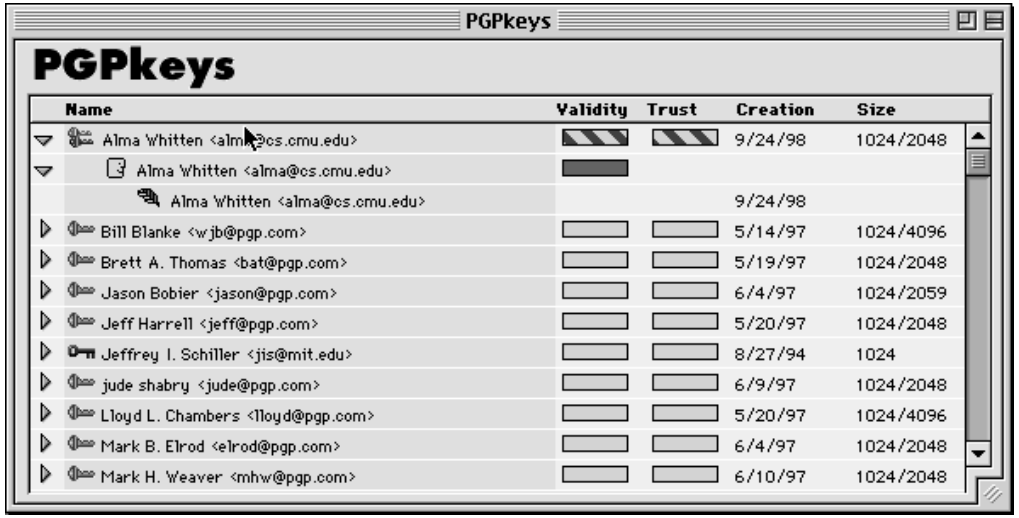
Tradeoff between usability and security

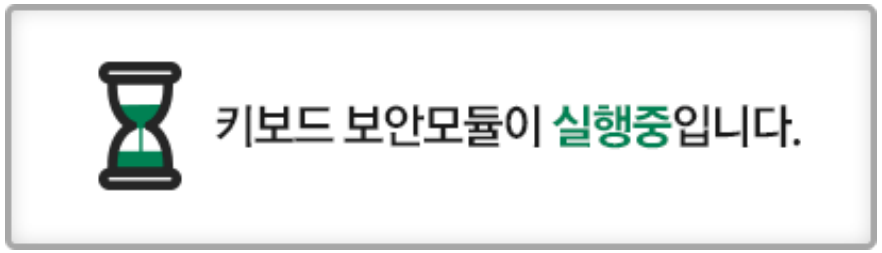
Secure
Difficult to use

Where is the best position?

Easy to use
Insecure







Security Theater?
The practice of investing in countermeasures intended to provide the feeling of improved security while doing little or nothing to actually achieve it

Conclusion

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