The origins: The three classic papers on usable security

The classics

- Whitten & Tygar: Why Johnny Can’t Encrypt
- Adams & Sasse: Users Are Not the Enemy
- Good & Krekelberger: Usability and privacy: a study of Kazaa P2P file-sharing

Why classics?

- Early papers on the topic (1999, 1999 & 2003)
- Present
  - a definition for usable security widely referred to
  - the basic problems in usable security
  - the idea of studying security with HCI methods

Why Johnny Can’t Encrypt

- Authors
  - Doug Tygar – security prof. at UCB
  - Alma Whitten – grad student of Tygar
    - A reading list on usable security
    - Now at Google
  - Not active on usable security since

- Paper came out at USENIX security which is a technical conference

Why Johnny Can’t Encrypt

- The paper presents a usability study of PGP 5.0
  - Claimed to have good usability
  - ”can be successfully used by cryptography novices to achieve effective electronic mail security”
  - The authors suspected the claim so they tested it

The user study

- cognitive walkthrough analysis together with
- a laboratory user test
- test participants were given 90 minutes in which to sign and encrypt a message using PGP 5.0
- the majority of them were unable to do so successfully

Definition: 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

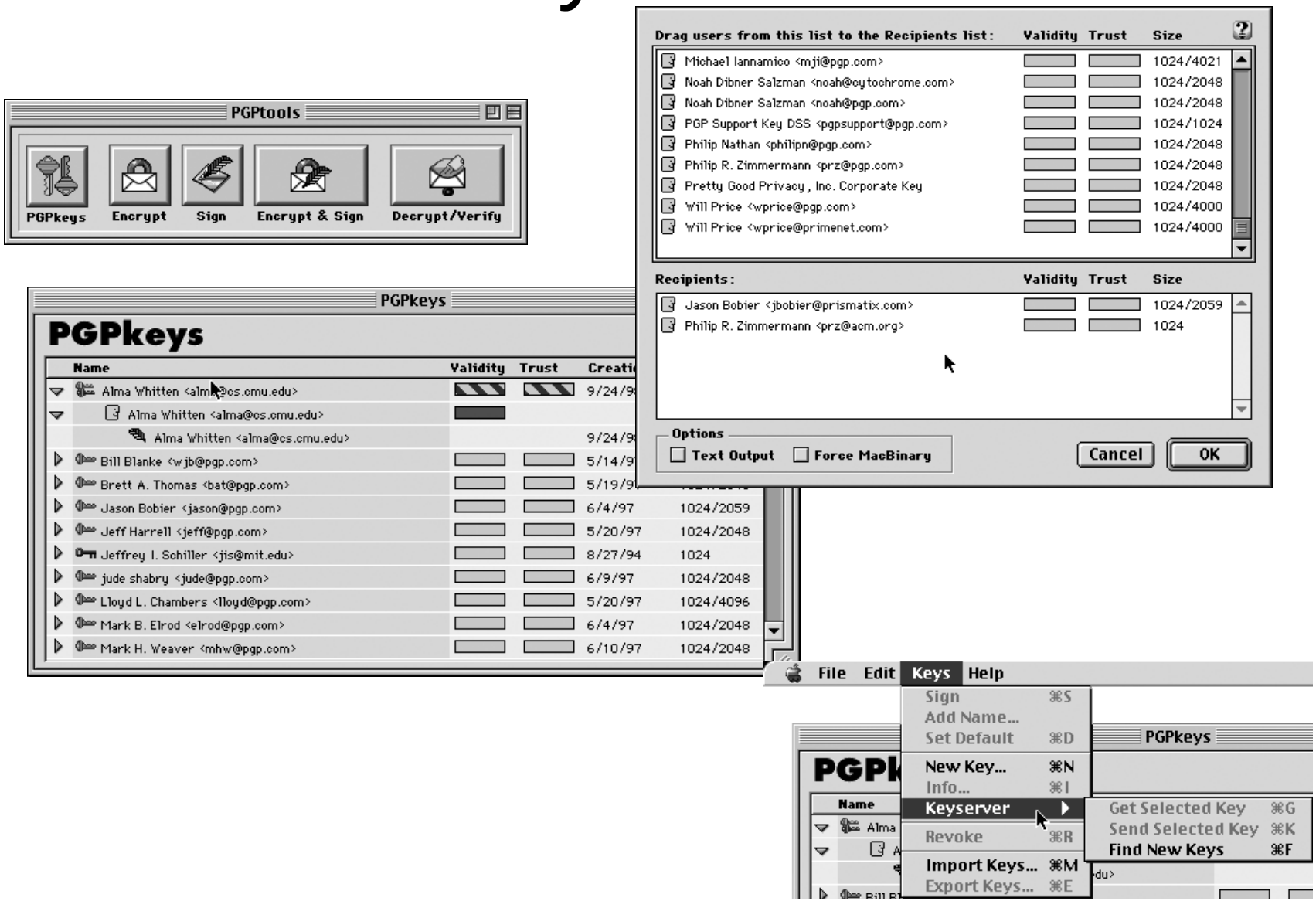
Problematic Properties of Security

- The unmotivated user property
- The abstraction property
- The lack of feedback property
- The barn door property
- The weakest link property

In order to PGP to be usable, users can…

- Understand that privacy is achieved by encryption, and figure out how to encrypt email and how to decrypt email received from other people
- Understand that authentication is achieved through digital signatures, and figure out how to sign email and how to verify signatures on email from other people
- Understand that in order to sign email and allow other people to send him encrypted email, a key pair must be generated, and figure out how to do so
- Understand that in order to allow other people to verify his signature and to send him encrypted email, he must publish his public key, and figure out some way to do so
- Understand that in order to verify signatures on email from other people and send encrypted email to other people, he must acquire those people's public keys, and figure out some way to do so
- Manage to avoid such dangerous errors as accidentally failing to encrypt, trusting the wrong public keys, failing to back up his private keys, and forgetting his passphrases
- Be able to succeed at all of this within a few hours of reasonably motivated effort

The fancy UI


PGPtools
PGPkeys
Encrypt
Sign
Encrypt & Sign
Decrypt/Verify
Drag users from this list to the Recipients list:
Validity
Trust
Size
Michael Iannamico <mji@pgp.com> 1024/4021
Noah Dibner Salzman <noah@cytochrome.com> 1024/2048
Noah Dibner Salzman <noah@pgp.com> 1024/2048
PGP Support Key DSS <pgpsupport@pgp.com> 1024/1024
Philip Nathan <philipn@pgp.com> 1024/2048
Philip R. Zimmermann <prz@pgp.com> 1024/2048
Pretty Good Privacy, Inc. Corporate Key 1024/2048
Will Price <wprice@pgp.com> 1024/4000
Will Price <wprice@primenet.com> 1024/4000
Recipients:
Jason Bobier <jbobier@prismatix.com> 1024/2059
Philip R. Zimmermann <prz@acm.org> 1024
Options
Text Output
Force MacBinary
Cancel
OK
PGPkeys
Name
Validity
Trust
Alma Whitten <alma@cs.cmu.edu>
Bill Blanke <wjb@pgp.com> 5/14/9
Brett A. Thomas <bat@pgp.com> 5/19/9
Jason Bobier <jason@pgp.com> 6/4/97 1024/2059
Jeff Harrell <jeff@pgp.com> 5/20/97 1024/2048
Jeffrey I. Schiller <jis@mit.edu> 8/27/94 1024
jude shabry <jude@pgp.com> 6/9/97 1024/2048
Lloyd L. Chambers <lloyd@pgp.com> 5/20/97 1024/4096
Mark B. Elrod <elrod@pgp.com> 6/4/97 1024/2048
Mark H. Weaver <mhw@pgp.com> 6/10/97 1024/2048
File
Edit
Keys
Help
Sign ⌘S
Add Name...
Set Default ⌘D
New Key... ⌘N
Info... ⌘I
Keyserver
Revoke ⌘R
Import Keys... ⌘M
Export Keys... ⌘E
Get Selected Key ⌘G
Send Selected Key ⌘K
Find New Keys ⌘F

Outcomes and Analysis

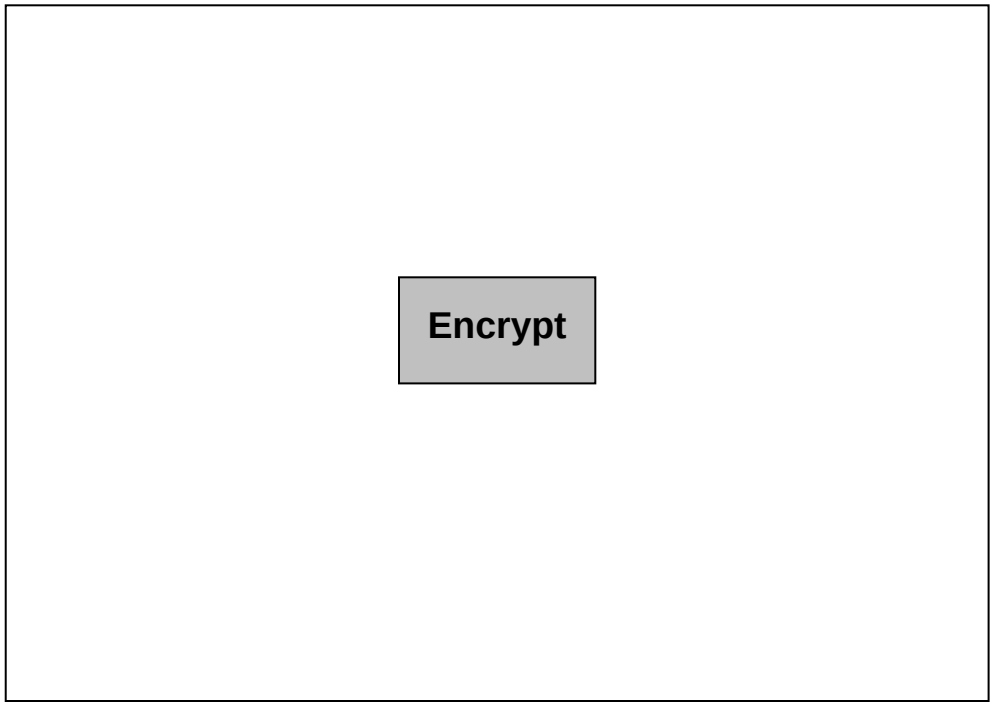
- Users were mostly unable to perform
- As remedy, authors suggest more usability work to back up the claims of easy to use
- Point out the importance of good visual metaphors
- …and need for clear task flow.

However…

Instead of..

- Understand that privacy is achieved by encryption, and figure out how to encrypt email and how to decrypt email received from other people
- Understand that authentication is achieved by digital signatures, and figure out how to sign email and how to rely on email from other people
- Understand that in order for people to send him encrypted email, he needs to figure out how to do so
- Understand that in order to verify a signature and to send him encrypted email, people need to find and figure out some way to do so
- Understand that in order to get other people and send encrypted email to them, people need to get people's public keys, and figure out some way to do so
- Manage to avoid such things as accidentally failing to encrypt, trusting the wrong public key, losing track of his private keys, and forgetting his passphrase
- Be able to succeed at all of these within a few hours of reasonably motivated effort

Why not just…



Problems with the paper

- Went along with the technology instead of thinking outside the box
- Users become slaves to the task at hand
- Too much technology is shown to the user
- UI mimics the encryption steps unnecessarily

Some additional classic ingredients in the paper

- Discuss double expertise (domain expertise + usability expertise)
- Discuss test setting & security awareness
- Use mixed-methods approach

Users are not the enemy

- Authors
  - Angela Sasse – HCI professor at UCL
  - Anne Adams – grad student of Sasse
    - Now researcher at Open University
- Paper came out at CACM

  → Big impact

Users are not the enemy

- ***Why users compromise computer security mechanisms and***
- ***how to take remedial measures.***
- ***A study on Password security in the organizational context (= workplace)***

Methodology

- A Web-based questionnaire was used to obtain initial quantitative and qualitative data on user behaviors and perceptions relating to password systems.
  - password related user behaviors (password construction, frequency of use, password recall and work practices) and in particular memorability issues.

- The questionnaire was followed by 30 semistructured in-depth interviews with some respondents
  - password generation and recall along with systems and
  - organizational issues raised by respondents in the questionnaire.

Outcomes

Four major factors influencing effective password usage were identified

- Multiple passwords;
- Password content;
- Perceived compatibility with work practices; and
- Users' perceptions of organizational security and information sensitivity.

“Constantly changing passwords forced me to make very simple choices that are easy to guess, or break…Hence there is no security.”

“…security problems are more by word of mouth…”.

“…because I was forced into changing it every month
I had to write it down.”

“I don’t think that hacking is a problem—I’ve
had no visibility of hacking that may go on. None at
all.”

“I would
have thought that if you picked something like your
wife’s maiden name or something then the chances of
a complete stranger guessing *********, in my case,
were pretty remote.”

“I cannot remember my password, I have to write it down,
everyone knows it’s on a post-it in my drawer, so I might as well stick it on the screen and tell everyone
who wants to know.”

Analysis

- Insufficient communication with users produces a lack of user-centered design in security mechanisms
- Users can be motivated if given the information in the right way
- Organizational structures often prohibit users from getting this info and from participating in the security process.

What makes it a classic

- Attacking the traditional (and unquestioned) claim that users are just ignorant and unmotivated (they often are, but that’s not the whole story)
- Showcasing the organizational problems in maintaining security when users need to be involved

Usability and privacy: a study of Kazaa P2P file-sharing

- Authors
  - Nathan Good – then at HP, now at UCB
  - Aaron Krekelberg – then at HP, now ?

- Paper presented at CHI

  →Good impact for usability community

?

What’s the paper about

- a cognitive walkthrough as well as
- a laboratory user study to analyze
- the usability of the Kazaa file sharing user interface.

Outcomes

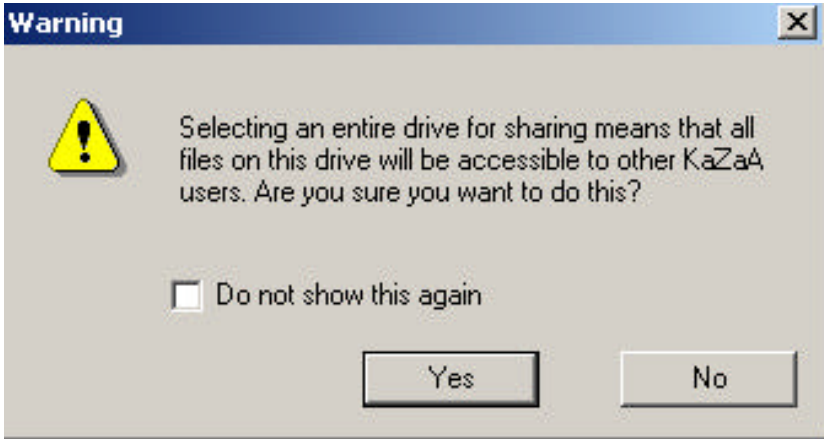
- majority of the users in the study were unable to
  - tell what files they were sharing, and
  - sometimes incorrectly assumed they were not sharing any files
  - when in fact they were sharing all files on their hard drive.
  - Only 2 of the 12 users were able to determine correctly the files and folders that were being shared.
- Also examined the current Kazaa network, and determined that
  - a large number of users were sharing personal and private files without their knowledge
- Were also able to see from a dummy server that
  - other users were taking advantage of this and downloading files such as "Credit Cards.xls" and email files.

Recommendations by the authors

1. *Users should be made clearly aware of what files are being offered for others to download.*
2. *Users should be able to determine how to successfully share and stop sharing files.*
3. *Users should not be able to make dangerous errors that can lead to unintentionally sharing private files.*
4. *Users should be sufficiently comfortable with what is being shared with others and confident that the system is handling this correctly*

Why this paper is important

- Able to show **how little aware users were** of their privacy status
- Raised the issue on the importance of **good defaults** for security and privacy
- …and on **not allowing dangerous options.**



Next lecture

- 1.2. Topic: Trust