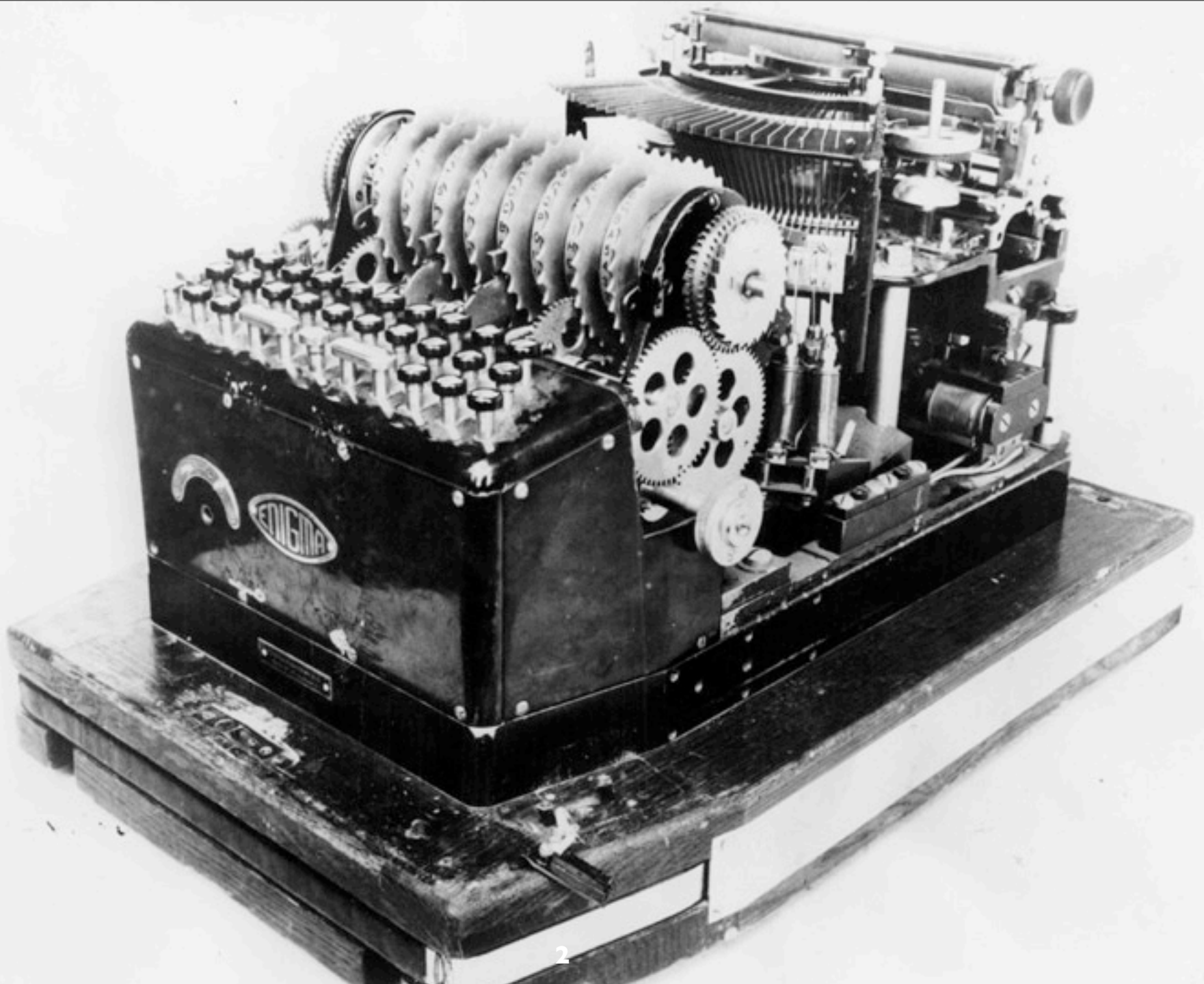


# Security and Human Factors



Maritza Johnson  
[maritzaj@cs.columbia.edu](mailto:maritzaj@cs.columbia.edu)



2

# Usability

“the extent to which a product can be used by **specified users** to achieve **specified goals** with effectiveness, efficiency and satisfaction in a **specified context of use**”

ISO 9241-11

# Principles of Information Protection

- Psychological acceptability
- Fail-safe defaults (default deny)
- Least privilege
- Separation of privilege
- Least common mechanism
- Complete mediation
- Open design
- Economy of mechanism

J. Saltzer and M. Schroeder, "The Protection of Information in Computer Systems," *Proceedings of the IEEE* 63:9 (1975), 1278-1308.

# Psychological acceptability

- Designed for ease of use
- Routine, automatic, correct
- Accurate mental model

J. Saltzer and M. Schroeder, "The Protection of Information in Computer Systems," *Proceedings of the IEEE* 63:9 (1975), 1278-1308.



# Secure but not Usable

- Can the user intentionally subvert your security mechanisms?
- Can they unknowingly influence the effective security?

# Usable but Not Secure

- Can the user accomplish their tasks?
- Is performance affected?



- Is the user aware of the security tasks they need to perform?
- Is the user equipped to successfully perform those tasks?
- Is it possible for the user to make dangerous errors?
- Will the user be sufficiently comfortable with the interface to continue using it?

A. Whitten and J.D. Tygar, Why Johnny Can't Encrypt: A Usability Case Study of PGP 5.0. Proceedings of the 8th USENIX Security Symposium, August 1999.

# Complicating Factors

- Unmotivated user
- Lack of feedback
- Abstraction
- Weakest link
- Barn door

A. Whitten and J.D. Tygar, Why Johnny Can't Encrypt: A Usability Case Study of PGP 5.0. Proceedings of the 8th USENIX Security Symposium, August 1999.

# A Few Usable Security Topics

- Encrypted email
- Passwords
- Phishing
- Wi-Fi
- Firewall policy management
- File access control
- Privacy settings

# Encrypted Email

- Public/private key metaphor
- How to select the correct key?
- Feedback?
- Johnny 2

# Passwords

- Acceptable to users
- Cheap and easy to deploy
- Minimal maintenance costs

# Password Policies

- Use upper and lower-case letters, numerical digits, and special characters
- Do not use words found in a dictionary
- Must be at least 6-8 characters long
- Never write down or share your password
- Change your password whenever there is suspicion they may have been compromised
- Never reuse a password for more than one account
- Make passwords COMPLETELY random but easy for you to remember

- What is your pet's name?
- Where were you born?
- What is your favorite restaurant?
- What is the name of your school?
- Who is your favorite singer?
- What is your favorite film?
- Where was your first job?
- Where did you grow up

“The hacker guessed that Alaska's governor had met her husband in high school, and knew Palin's date of birth and home zip code. Using those details, the hacker tricked Yahoo Inc.'s service into assigning a new password, "popcorn," for Palin's e-mail account”

[http://www.huffingtonpost.com/2008/09/18/palin-email-hacker-impers\\_n\\_127538.html](http://www.huffingtonpost.com/2008/09/18/palin-email-hacker-impers_n_127538.html)



# Password Usability Problems

- People are bad at generating random strings
- They're not good at remembering them
- Managing several passwords is difficult
- Most people don't know what makes a password "good"


[10] Woodgrove Account Violation

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next

**From:** Account Notice  
**Date:** Wed, 8 Sept 2004 12:41p  
**To:**  
**Subject:** [10] Woodgrove Account Violation

**WOODGROVE BANK** MEMBER EDIT

Dear valued Woodgrove member,  **Graphic from bank's actual web site**

In our terms and conditions you have agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have tried gaining access or control of your information in your account.

Therefore, to prevent unauthorized access to your Woodgrove Internet Banking account, you are limited to five failed login attempts in a 24-hour period. You have exceeded this number of attempts.\*

Please follow the link below and renew your account information.

<https://vault.woodgrove.com/default.asp> <sup>1</sup>

<http://203.144.234.138/us/index.html> <sup>2</sup>

# Advice to Users

- Look for the lock
- Look for “https”
- Check the URL
- Do not click on links in emails

# Usability Problems

- Inaccurate mental model
- Inability to parse URLs
- Phishing websites use SSL
- The scam exploits human emotion

## If your SiteKey is correct, you know you are at the valid Bank of America site.

---

If you recognize your SiteKey, please enter your passcode and click the **Sign In** button.

An asterisk (\*) indicates a required field.

Your SiteKey:



my private message

\* Passcode:

(4-12 numbers and/or letters, case sensitive)

**Sign In**

## If your SiteKey is correct, you know you are at the valid Bank of America site.

---

If you recognize your SiteKey, please enter your passcode and click the **Sign In** button.

An asterisk (\*) indicates a required field.

Your SiteKey:



my private message

\* Passcode:

(4-12 numbers and/or letters, case sensitive)

**Sign In**

**Website Identification**

VeriSign has identified this site as:

VeriSign, Inc.  
Mountain View, California  
US

This connection to the server is encrypted.

Should I trust this site?

[View certificates](#)



Purchase S

### Select certificate options

Changing your certificate options may c

ptions, click **Recalculate** to see the new price.

#### Product: SSL Secure Site Pro

SSL Certificate with SGC, Business Authentication, \$250,000 (or equivalent in local currency) of NetSure Protection, Keynote Red Alert Accessibility Evaluation, Netcraft E-Commerce Security Analysis (\$1,000 value), Qualys Network Security Auditing Service, VeriSign Secured Seal, Free 30-Day SSL Certificate Revocation and Replacement. [2-day Express Delivery](#)

**Added Options:** Two Year Validity Period

**Total: US\$ 1,790**

# Wi-Fi

- Is the network trusted?
- Is the network encrypted?
- What type of websites do users visit?

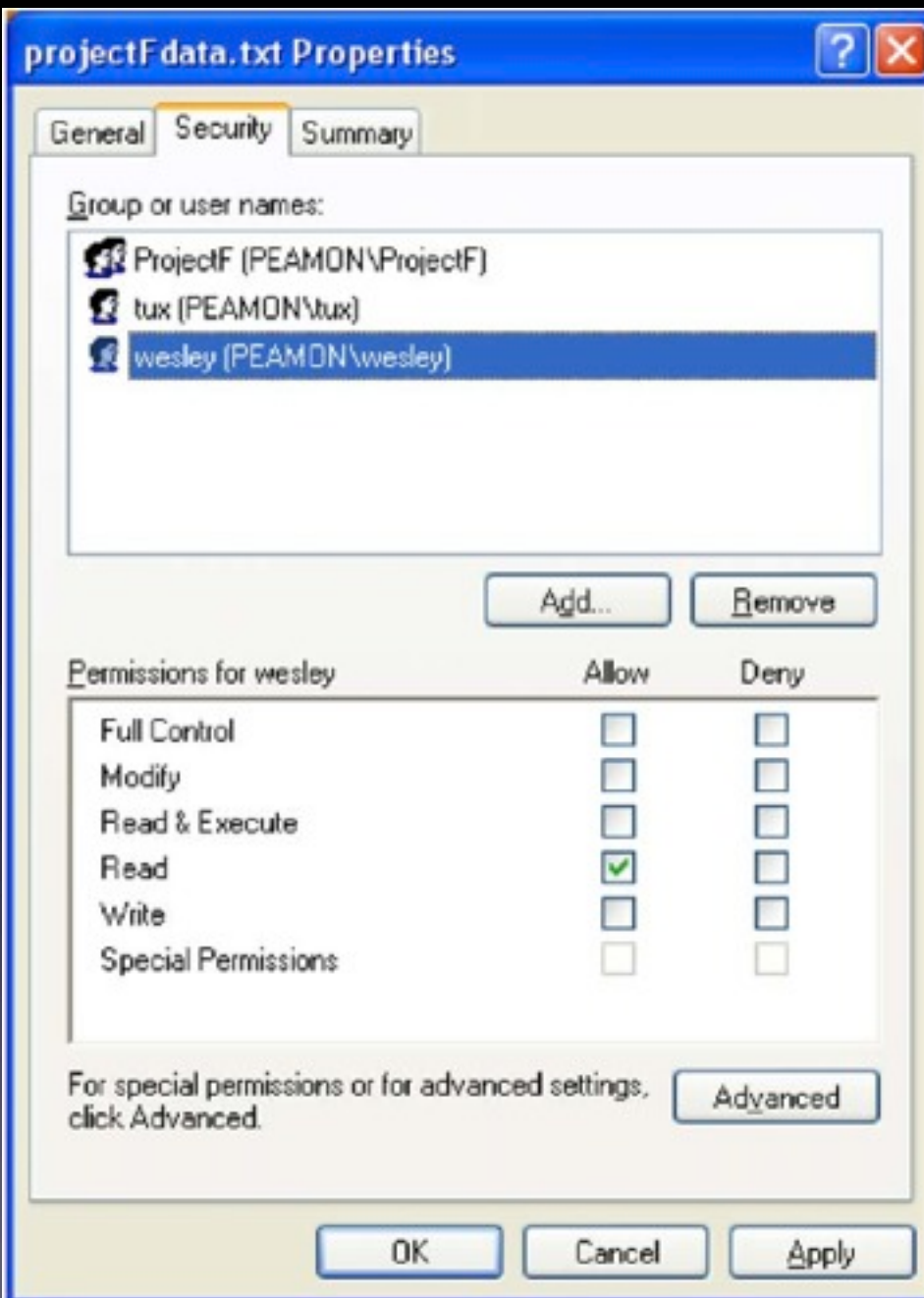


# Firewall Policy Management

- A list of allow/deny rules
- Rule order usually matters
- Frequent changes
- Rules expire

# File Access Control

- How do I grant read or write permissions to another user?
- How do I know who can access which resources?
- And what do they have permission to do?







## Privacy ▸ Profile



Basic Contact Information

Control who can see which sections of your profile. Visit the [Applications page](#) in order to change settings for applications. Visit the [Search Privacy page](#) to make changes to what people can see about you if they search for you.



See how a friend sees your profile:


Profile  Only Friends  [?]

Basic Info  Only Friends  [?]



Personal Info  Only Friends  [?]

Status and Links  Only Friends  [?]

Photos Tagged of You  Custom  [?]



 Can See Pics

[Edit Custom Settings](#)

Videos Tagged of You  Custom  [?]

 Can See Pics

[Edit Custom Settings](#)

Friends  Only Friends  [?]



# Designing for Usable Security

- Know your user
  - Background
  - Abilities
  - Limitations
- Know the user's goals and tasks

# Designing for Usable Security

- Consider environmental factors that may affect user behavior
- Design for robustness against potential attacks
  - Spoofability
  - Information overload
  - Warning fatigue


# General Guidelines

- Make the default settings secure
- Use automation when possible
- Don't “punt” to the user when a problem arises



- Does it behave correctly when not under attack?
- Does it behave correctly when under attack?
- Can it be spoofed, obscured, or otherwise manipulated?
- Do users notice it?
- Do the users know what it means?
- Do users know what they are supposed to do when they see it?
- Do they actually do it?
- Do they keep doing it over time?
- How does it interact with other indicators that may be installed on a user's computer?

<https://mail.google.com/>

mail.google.com 

- Does it behave correctly when not under attack?
- Does it behave correctly when under attack?
- Can it be spoofed, obscured, or otherwise manipulated?
- Do users notice it?
- Do the users know what it means?
- Do users know what they are supposed to do when they see it?
- Do they actually do it? Do they keep doing it over time?
- How does it interact with other indicators that may be installed on a user's computer?

## Security Alert



Information you exchange with this site cannot be viewed or  
ite's

There is a problem with the  
site's security certificate

u have  
whether

The security certificate was  
issued by a company you have  
not chosen to trust

e you

Do you want to proceed?

Yes

No

View Certificate

## Security Alert



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.



The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.



The security certificate date is valid.



The security certificate matches the name of the page you are trying to view.

Do you want to proceed?

**YES!**

No

View Certificate

# Designing Warning Messages

- Use a warning appropriate to the situation
- Clearly state the situation in natural language
- Ask the question in context
- Give the user reasonable choices to resolve the issue



## Reported Attack Site!

This web site at ianfette.org has been reported as an attack site and has been blocked based on your security preferences.

Attack sites try to install programs that steal private information, use your computer to attack others, or damage your system.

Some attack sites intentionally distribute harmful software, but many are compromised without the knowledge or permission of their owners.

Get me out of here!

Why was this site blocked?

[Ignore this warning](#)

# Evaluation Methods

- Low fidelity prototyping
- Interviews
- Focus groups
- Heuristic evaluation
- Cognitive walk-through

# Evaluation Methods

- Laboratory studies
- Field studies
- Ethnographic studies



# Usability Testing

- Is there a human in the loop?
- Who do you use for participants?
- What do you ask them to do?
- Under what conditions?

# Phishing User Studies

- “Why Phishing Works”
- “The Emperor's New Security Indicators”
- “Designing and Conducting Phishing Experiments”
- “School of Phish: A Real-World Evaluation of Anti-Phishing Training.”

# IRB: Institutional Review Board

- A committee that reviews research projects involving human subjects
- Minimize risk
- Informed consent
- <http://www.rascal.columbia.edu>

# Summary

- Usability is important!
- Many open topics
- Design guidelines
- Evaluation techniques and design

HCISec Bibliography

<http://www.gaudior.net/alma/biblio.html>

Usable Security Blog

<http://usablesecurity.com/>

Symposium on Usable Privacy and Security

<http://cups.cs.cmu.edu/soups/>

HCI Bibliography

<http://www.hcibib.org/>