Security and the Human Factor

- **Today:**
  - Users as the enemy
  - Social engineering attacks

- **Next time:**
  - When to design for usability
Usability & Security

- Traditional focus of “security” in information systems: features or properties of the *system*
  - Software bugs, cryptographic protocols, …

- What is information security? (reminder)
  - Protecting information systems against misuse and interference
  - “Building systems to remain dependable in the face of malice, error or mischance” (Ross Anderson)

- Design goals of a system almost always (perhaps implicitly) include humans as part of that system
  - Features are no good if people can’t use them
  - A system isn’t secure if users always make mistakes

- For practical definitions of security, a system cannot be “secure” unless it is usable
What Can Make a System Not Usable?

- Confusing / misleading / unhelpful user interface
- Requiring users to make decisions for which user is not qualified
- Assuming knowledge or abilities that user doesn’t have
- Assuming unreasonable amount of attention / effort
Example

Example: Warning Dialogs

- Why is this a bad user interface?
  - No clear statement of risk (e.g., “The server might not be who it claims”)
  - Missing explanation of consequences (e.g., “A third party could gain access to the information you create or share with this application”)
  - No instructions on how to make situation better (e.g., “Check the certificate and decide if you trust this site…”)
Example: Warning Dialogs

- **Why is this a bad user interface?**
  - No clear statement of risk (e.g., “You may be disclosing private information to this application”)
  - Missing explanation of consequences (e.g., “This application will have full access to your calendar”)
  - No instructions on how to make situation better (e.g., “If you were expecting this application to access your calendar…”)
Example: Warning Dialogs

- Guidelines for more usable warning design
  - Describe risk comprehensively
  - Be concise and accurate
  - Offer meaningful options
  - Don’t use jargon
  - ...

- Better yet: remove warning if at all possible
  - Design system so that user doesn’t need to be bothered with confusing, difficult decisions
Admins Are Users Too
Example: Setting Access Control Rules
Example: Setting Access Control Rules

[Diagram of Access Control window with groups and permissions listed]
Example Task – Jana

- Scenario: You are a TA in a Music department and have to maintain the department file server.

- Task:
  Jana, a Music Theory 101 TA, complained that when she tried to change the Four-part Harmony handout to update the assignment, she was denied access.

Set permissions so that Jana can read and write the *Four-part Harmony.doc* file in the *Theory 101/Handouts* folder.
Example Task Setup

- Jana is the TA “this” year (2007)
  - Is in the group “Theory 101 TAs 2007
- Jana was a TA last year
  - Is in the group “Theory 101 TAs 2006
- 2007 TAs are allowed read and write
- 2006 TAs are denied read and write
- Since Jana is in both groups, she is denied access
Jana Task – Common Error
Learning Jana’s Effective Permissions

1. Click “Advanced”
2. Click “Effective Permissions”
3. Select Jana
4. View Jana’s Effective Permissions
Learning Jana’s Group Membership

1. Bring up Computer Management interface

2. Click on “Users”

3. Double-click Jana

4. Read Jana’s group membership

5. TAs 2006

6. TAs 2007

7. Click “Member Of”

8. Double-click Jana

9. Read Jana’s group membership
Learning Jana’s Groups’ Permissions

10. Click on TAs 2006

11. Read permissions for TAs 2006

12. Read permissions for TAs 2007

13. Click on TAs 2007
Changing Jana’s Groups’ Permissions

14

Click on TAs 2006

15

Change permissions for TAs 2006
Checking Work

16. Click "Advanced"

17. Click "Effective Permissions"

18. Select Jana

19. View Jana’s Effective Permissions
A Better Interface?
Birthday Party Permission Error

- A girl in Germany created a Facebook event for her sweet 16 birthday
- Event was public and went viral
- 15,000 RSVP'd
- 1,600 showed up

[ http://www.cbsnews.com/8301-504083_162-20069457-504083.html ]
Example: Password Policies

With the Spring 2014 release, *myPay* will be updating its system password rules that meets the intent of DoD security policies and customer feedback. This means all users who access *myPay* with their login ID and password must create a new password using the following rules:

- Must be 9 to 30 characters in length
- Contain at least one UPPERCASE letter
- Contain at least one lowercase letter
- Contain at least one number (0-9)
- Contain at least one of the following special characters:
  
  # (pound or number sign)
  @ (at sign)
  $ (dollar sign)
  = (equal sign)
  + (plus sign)
  % (percent sign)
  ^ (caret)
  ! (exclamation)
  * (asterisk)
  _ (underline/underscore)

- Must NOT include any spaces

Additionally, passwords will now expire every 150 days requiring users to change their passwords.
Example: Password Policies
An Exercise

Count the yellow squares
How Many Yellow Squares Are There?

27
How Many Yellow Squares Are There?

28
How Many Green Stars Are There?

The *real* question
How Many Green Stars Are There?

30
How Many Green Stars Are There?

31
Task: Check Your Account Balance
Why Usable Security Is Hard

- **Security is a secondary task for users**
  - Users trying to get something else done
  - ... don’t **want** to be spending time on security

- **Concepts are hard**
  - Encryption, keys, SSL, phishing, malware, ...

- **Human psychology**
  - Habituation to warnings
  - Limitations of memory
  - Attention focus
Attacks on or by Insiders

- “System” often includes both users and operators
  - Sysadmins, help desk, moderators

- Operators can also be a security risk
  - Higher permissions -> more risk of damage

- If “system” is secure, attack operators
Social Engineering Attacks: Example 1

- **Kevin Mitnick**
  - Early “hacker”
  - Convicted in 1999 of various computer-related crimes

- **Common attack techniques:**
  - Dumpster diving
  - Phoning help desk
  - Phoning admin, impersonating superior
Social Engineering Attacks: Example 2

- Christopher Hadnagy
  - Professional pen tester
  - “human hacker”

- **Common attack techniques:**
  - Impersonating superior or consultant, often in person
  - Impersonating someone in need of help
Attacks on or by Insiders: Takeaways

- Many categories of users
  - Special dangers due to insiders
  - Attackers can target the human element of the system

- Guidelines to minimize risk
  - Principle of least privilege
  - Written down processes for handling requests
  - Educate admins to refuse requests
  - Audit logs of security-relevant activity
Human Factor Takeaways

- A system must be usable to be secure
- Usability is *hard*
  - Hard concepts, hard-to-design interfaces, human limitations

- Insiders (operators / admins) are also users

- Next time: Can’t always add usability at the end