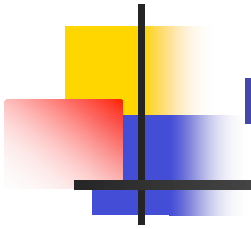
CSCI E-170
Computer Security, Usability & Privacy

Hour #1: Passwords



Identification, Authentication, and Authorization

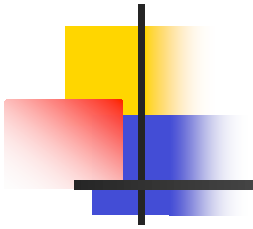
- Identification:
  - You give your name
- Authentication:
  - You've proven that it's really you.
- Authorization:
  - We've looked your identity up in the database and we know what you're allowed to do.
- Most say "authentication" when they mean identification or authorization.
- You can authenticate without identifying.

Classical Authentication

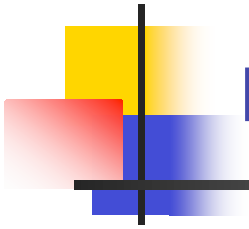
- Something that you know
  - password
  - pass phrases
- Something that you are
  - fingerprint
  - face print

  } biometrics
- Something that you have
  - tokens
  - smartcards

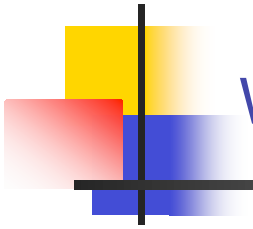
Passwords: What are they good for?



- Today passwords are the #1 means of authenticating users on a day-to-day basis.
  - Email, Websites, ATMs, Doors, Lockers, etc.
- Password Recovery:
  - Challenge/response questions
  - Knowledge of previous transactions



How many passwords do must you remember?

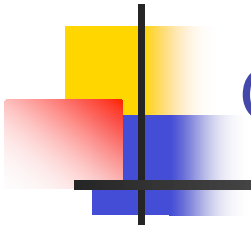


Why the explosion of passwords?

- Need to protect configuration information
  - BIOS passwords, VChip, Cell Phones, etc.
- Web services need persistent identification of users over time
- No national/international identification service

Alternatives to many passwords

- Single-sign on:
  - Master password unlocks others
  - PKI: password unlocks private key
- Examples:
  - Microsoft Passport
  - Gnu Keyring (gnukeyring.sourceforge.net)



Observed Strategies

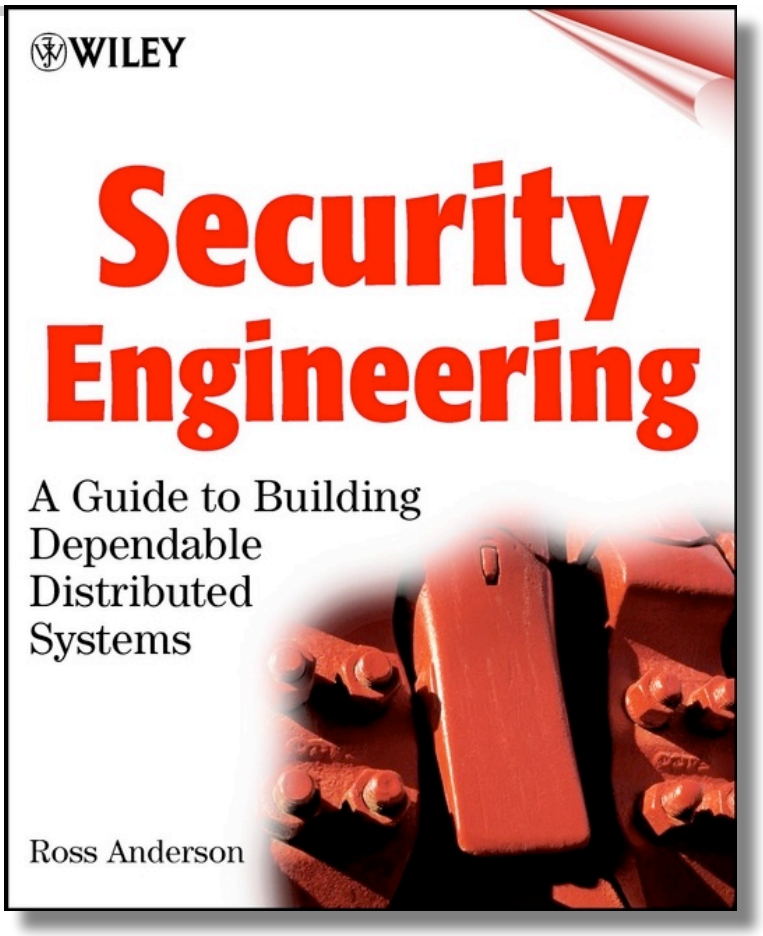
- “Low security” & “high security” passwords
- Standard password that’s changed for every host
  - password-ebay
  - password-paypall
  - password-fas
- Change password periodically
  - Every 3-6 months
  - (Problems if you don’t manage to change all of your passwords.)
- Always use “password reset” and get emailed a password.
- Write passwords down

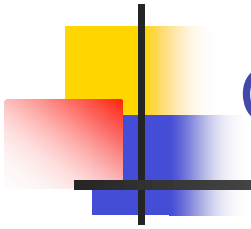
Anderson: 3 types of password concerns

Disclosure

Reliability to enter

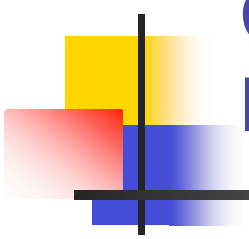
Ability to remember





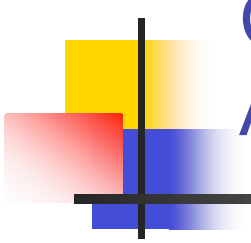
Concern #1: Disclosure

- Will the user break the system security by disclosing the password to a third party, whether accidentally, on purpose, or as a result of deception?



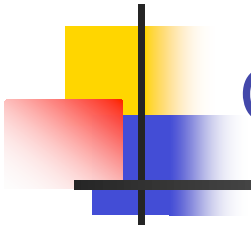
Concern #2: Reliability to enter

- Will the user enter the password correctly with a high enough probability?



Concern #3: Ability to remember

- Will users remember the password, or will they have to either write it down or choose one that's easy for the attacker to guess?

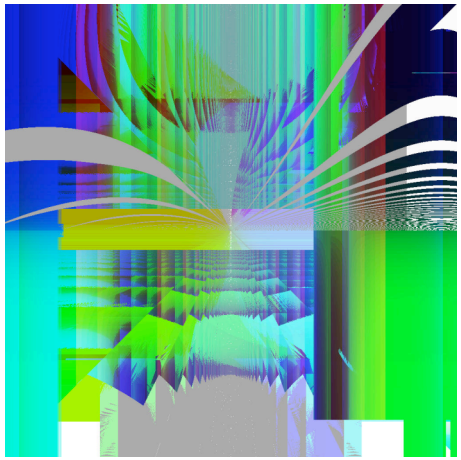


Can you write down passwords?

class discussion

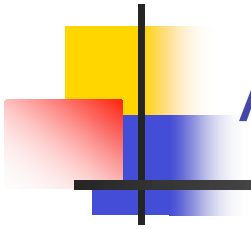
Can you write down these passwords?

Can you
remember them?



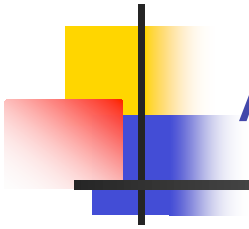
What if you had
to remember 40
of them?

http://gs2.sp.cs.cmu.edu/art/random/archive/archive_0104/



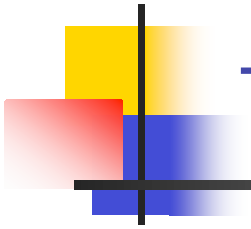
A Password Policy

- “The root password for each machine shall be too long to remember, at least 16 alpha and numeric characters chosen at random by the system;
- it shall be written on a piece of paper and kept in an envelope in the room where the machine is located;
- it may never be divulged over the telephone or used over the network;
- it may only be entered at the console of the machine that it controls.” [Anderson, p. 37]



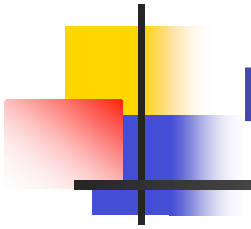
Anderson's Research Problems in Passwords:

- What is the best way to enforce user compliance with a password policy?
- Can we design interactive password systems that are better?
- Can we use multiple passwords?
  - Mother's maiden name
  - Password
  - Amount of last purchase
  - Dog's nickname
  - Your favorite color…



Threats to Passwords

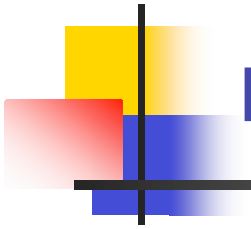
- What are the threats against passwords?
  - Guessing
  - Brute force search
  - Shoulder surfing
  - Discovering passwords that are written down
  - Passwords collected at one website used for another
- Kinds of attacks:
  - Offline
  - Online



Eavesdropping risks

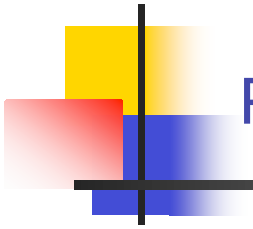
- Physical device --- key grabber
- Trojan Horse
- Tapped lines
- Video Camera

… The need for trusted path



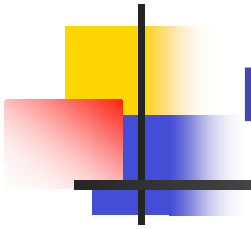
Kinds of Attacks:

- Targeted attack on one account
- Attempt to penetrate any account on a system
- Attempt to penetrate any account on any system
- Service denial attack



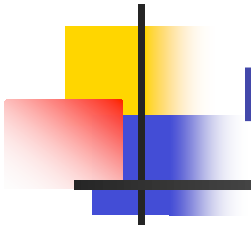
Protecting against Online Attacks:

- Defenses Against Guessing:
  - Exponential back-off
  - Lock out
  - Notification
  - “Cracking”
- Dangers of lock-out
  - eBay doesn’t use it; why not?



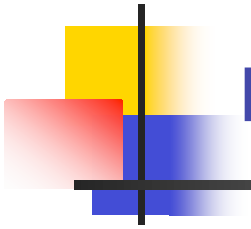
Protecting against Offline Attacks

- What do you do?
  - Prevent people from getting the encrypted database.
  - Make decrypting the database computationally difficult.



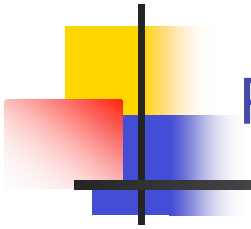
Restricting Passwords

- Does it make sense to mandate symbols and numbers in passwords?
  - # of letters: 52 (26 lower + 26 UPPER)
  - # of symbols: 30
  - # of 8 letter passwords: 52^8
  - # of 7 character passwords with 1 symbol: $(52^7)(30)(8)$
  - How about forcing 1 number and 1 symbol?
    - $(52^6)(30)(8)(10)(7)$
- But if you don't mandate it, people won't use them at all…



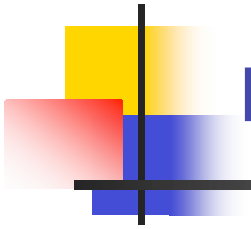
More on restrictions

- Different systems have different restrictions.
  - Some require special characters
  - Some forbid special characters.
- Why?
- Is this good or bad?
  - (I find it annoying, but that's because I want to use the same password on many different systems.)



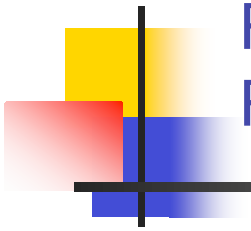
Password Generating Algorithms

- Multics generated passwords that were “easy to remember.”
- What’s wrong with giving advice on how to generate passwords?
- What’s the alternative?
- Programmatically picking passwords that are easy-to-remember



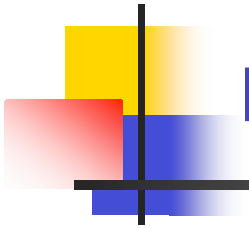
Developer Recommendations

- Force users to change passwords regularly
- Password != Username
- Require 8 or more characters
- Require a mix of alpha, numeric, and special characters
- Deny Access After a number of failed Attempts
- Do not send passwords “in the clear”
- Do not assign “default passwords”
- Overwrite passwords in memory as quickly as possible



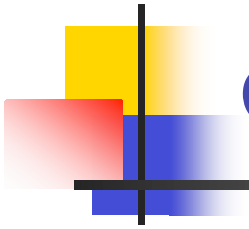
Restrictions on Passwords: Recommendations

- 1-14 characters vs. 1-127 characters vs. 10-127 characters
  - Recommendation: Mandate minimums, but allow people to type extra characters
  - If you can't handle a special character, change it to a character you can handle.
  - ATM networks used to ignore all characters after first 4



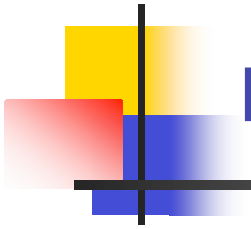
Recommendations on Password Aging:

- What should we do?
- Should we mandate password changes?
- Should we remember old passwords and forbid them?



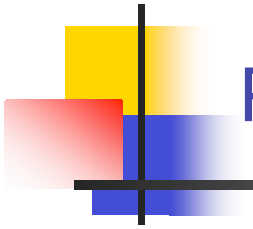
Case Sensitivity: Recommendations

- Some passwords are case-sensitive; some are not.
  - If your passwords are not case-sensitive, they must be longer.
- Check password with case-flipped for CAPS LOCK ON accident.



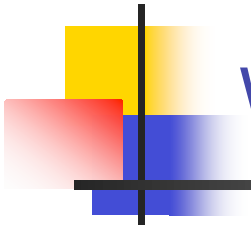
Password Recovery

- What's the best way to do it?
- Automatic vs. Manual
- "What is your favorite Color?"



Password Recovery: Recommendations

- Send a link that expires quickly.
- Specially log the IP address of the browser that clicks the link.
- Don’t send the password!



Web Password Hashing

- Internet Explorer plug-in that sends a hash of the password to every website.
  - Hash depends on your password & remote website
  - Defeats phishing!
- http://crypto.stanford.edu/PwdHash/
- http://crypto.stanford.edu/PwdHash/PwdHash.ppt