Technology: Protecting Yourself and Analyzing Impact on the CPC

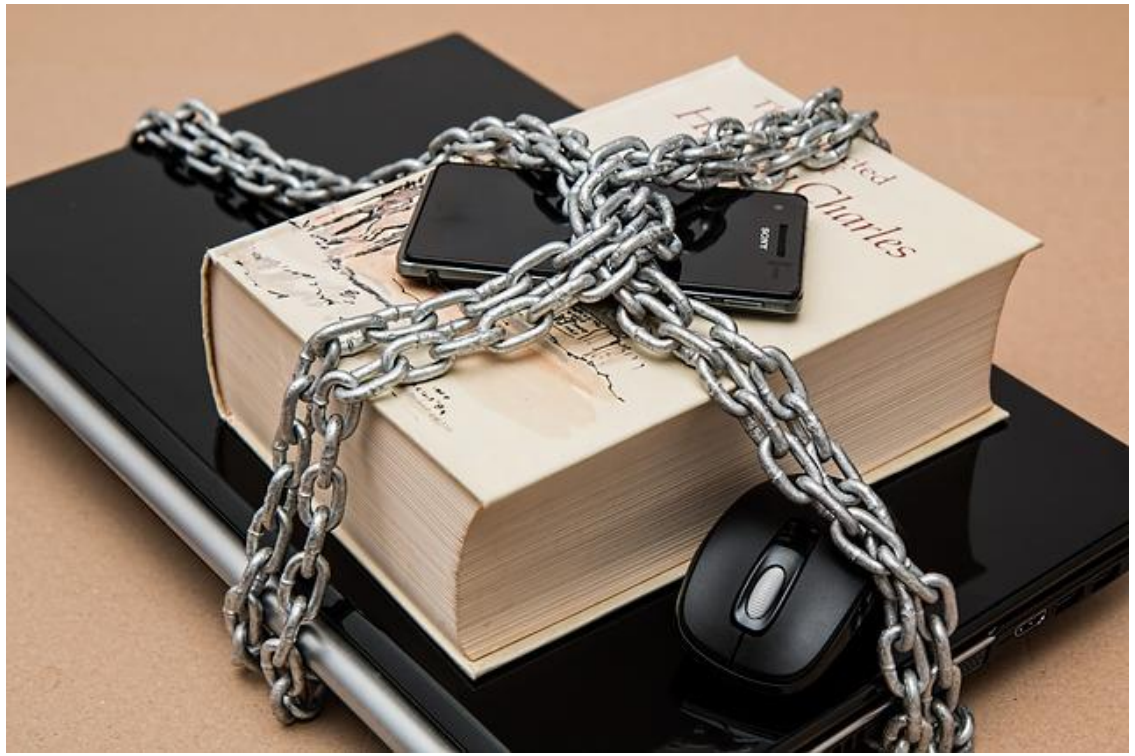
J. Michael Moore, PhD

Instructional Assistant Professor
Department of Computer Science and Engineering
Texas A&M University

Cybersecurity Breaches

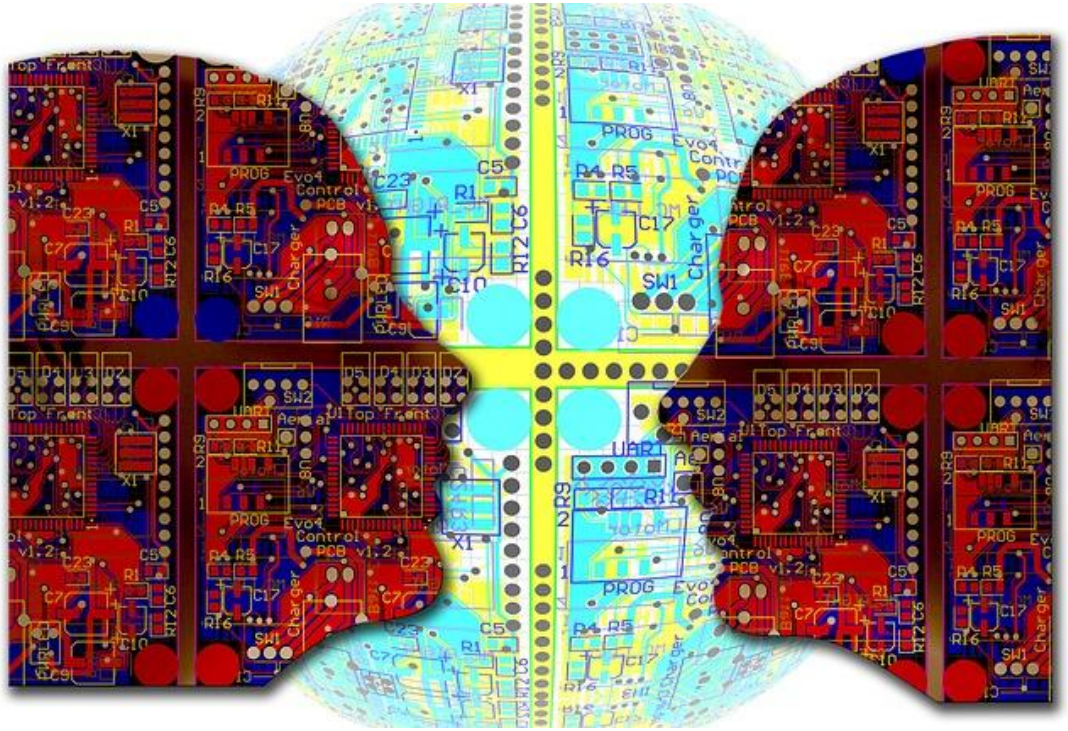
Goals

- Understand how technology works to guide its secure use.
- Examine how our use of technology in interpreting can impact the CPC.



Agenda

- Review CPC Tenants we will discuss.
- Discuss technology use and security strategies.
- Put it all together: Discuss the CPC in relation to technology that we use.



CPC Tenant - 1.0 CONFIDENTIALITY

Tenet: Interpreters adhere to standards of confidential communication.

Guiding Principle: Interpreters hold a position of trust in their role as linguistic and cultural facilitators of communication. Confidentiality is highly valued by consumers and is essential to protecting all involved.

Each interpreting situation (e.g., elementary, secondary, and post-secondary education, legal, medical, mental health) has a standard of confidentiality. Under the reasonable interpreter standard, professional interpreters are expected to know the general requirements and applicability of various levels of confidentiality. Exceptions to confidentiality include, for example, federal and state laws requiring mandatory reporting of abuse or threats of suicide, or responding to subpoenas.

Illustrative Behavior - Interpreters

1.1 Share assignment-related information only on a confidential and "as-needed" basis (e.g., supervisors, interpreter team members, members of the educational team, hiring entities).

1.2 Manage data, invoices, records, or other situational or consumer-specific information in a manner consistent with maintaining consumer confidentiality (e.g., shredding, locked files).

CPC Group Activity – Part A

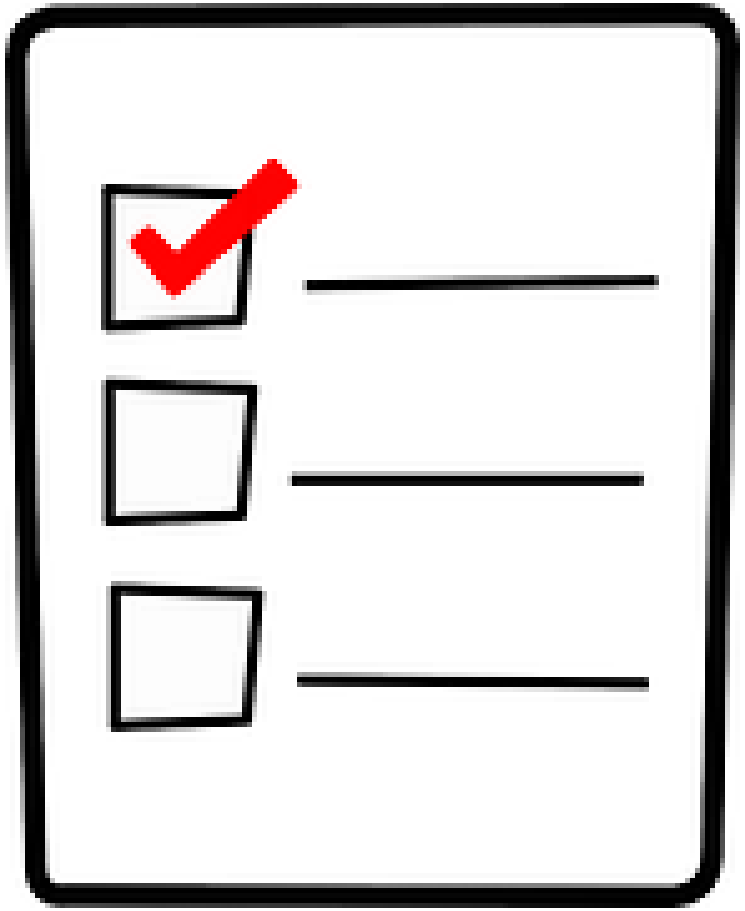
- 10 minutes
- Break into groups of 3 or 4 people.
- Select a reporter to record the results.
- Discuss ways in which technology might impact the CPC tenants presented.

Spam

- Unwanted messages
- Cheap
- Hard/Impossible to police
- Others?

Spam Email Verification

- **Reply**
- **Read your email**
  - HTML Images
- **Remove from list links**
  - If it’s a valid list this works
  - If it’s a spammer it doesn’t
- **Others?**



Spam Mitigation

- Do NOT Reply
- Block images for HTML email
- Use unsubscribe for legitimate lists
- Do NOT use unsubscribe for spam lists
- Spam filtering – Mark spam so the filter can learn
- Throw away addresses

- Others?

Social Engineering

- "in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information." -- Wikipedia

- "Why spend thousands of dollars on sophisticated hacking software when you could just trick someone into telling you the password?"

Social Engineering

- Tailgating
- Phishing
  - Spear Phishing
- Pretexting
- Baiting
- Quid Pro Quo

- 5 Social Engineering Attacks to Watch Out For

Link Analysis

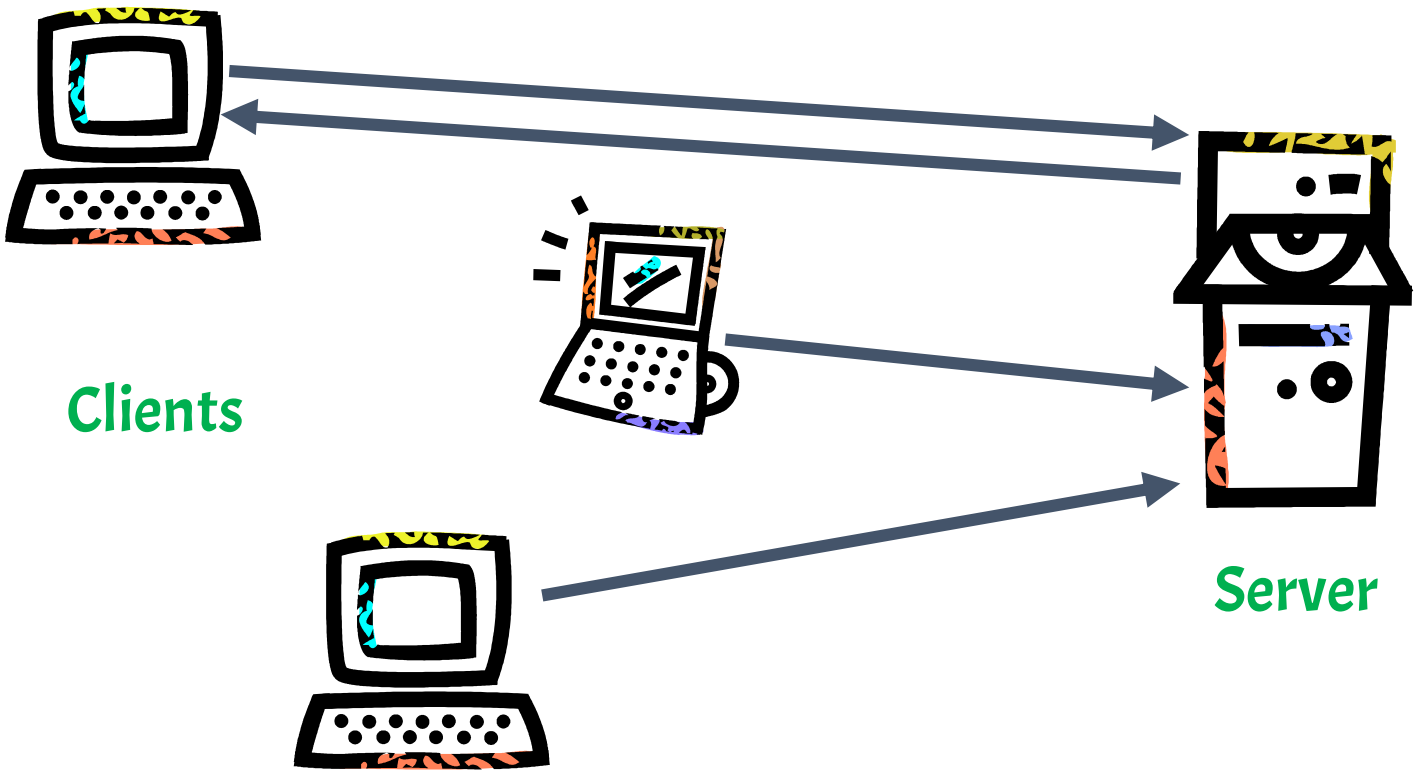
- **HTML Links**
  - Label : URL
  - http://www.tsid.org/stuff....
  - Examples

  - Get smart on Phishing! Learn to read links!

Social Engineering Group Activity

- 15 minutes discuss
- 10 minutes report
- Break into your groups
- Take turns discussing social engineering you have experienced that was hard to identify. Pick two to report to the group and explain how you can identify it.

Information Channels



Open

Encryption

"process of encoding messages or information in such a way that only authorized parties can read it." -- Wikipedia

Encrypted Path

Encrypted Data

Encrypted Data & Path

Automated Attacks

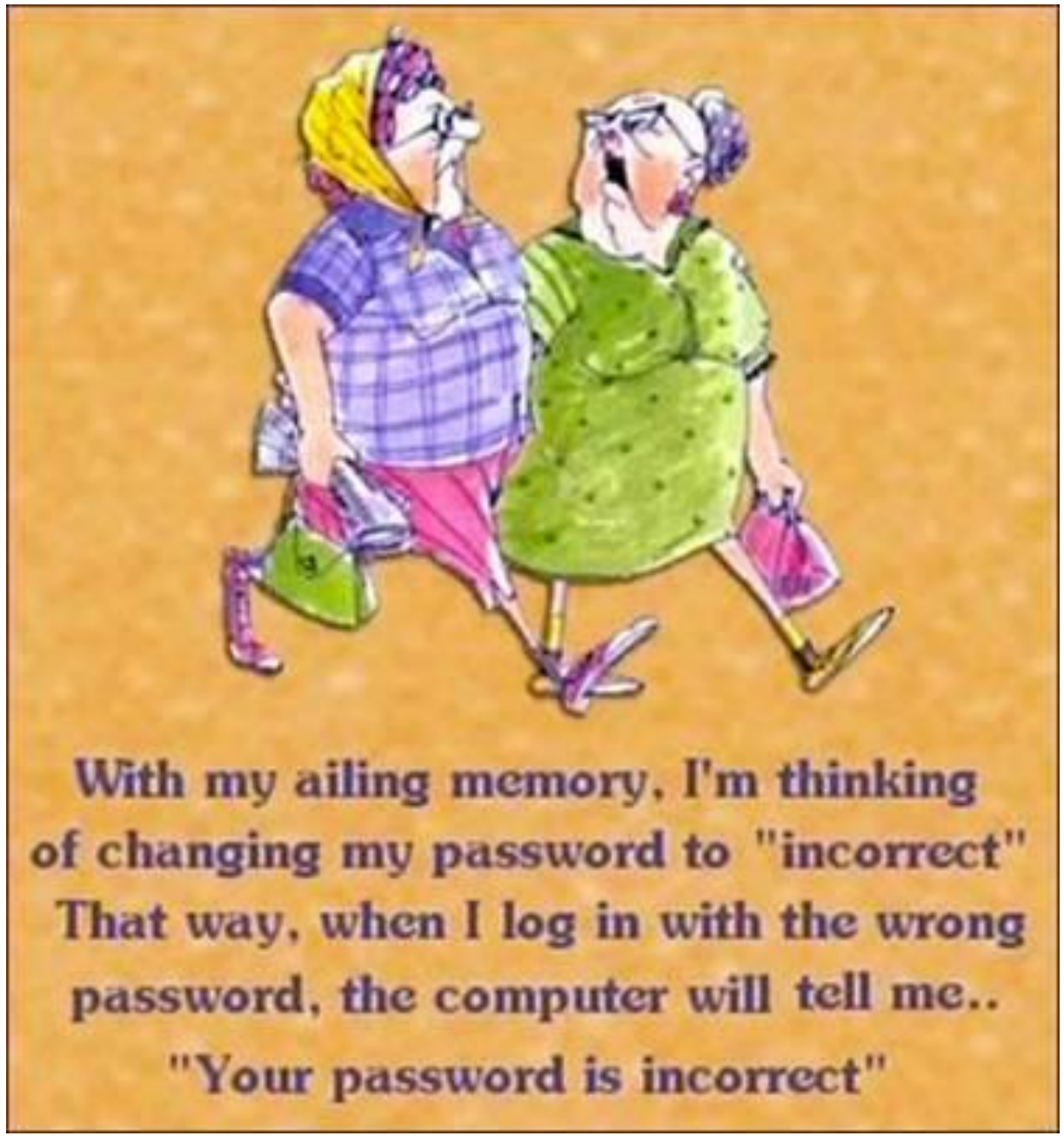
- **Guess Multiple Times**
  - Freeze login for a while
- **Brute Force…**
- **How to protect against automated attacks?**
  - Strong Passwords Help

Passwords

- **Traditional Strength Rules**
  - 12 characters (Minimum)
    - More is better
  - Includes numbers, special characters, lower and upper case letters
  - Isn’t a dictionary word or combination
  - Doesn’t rely on obvious substitutions

Password Notes

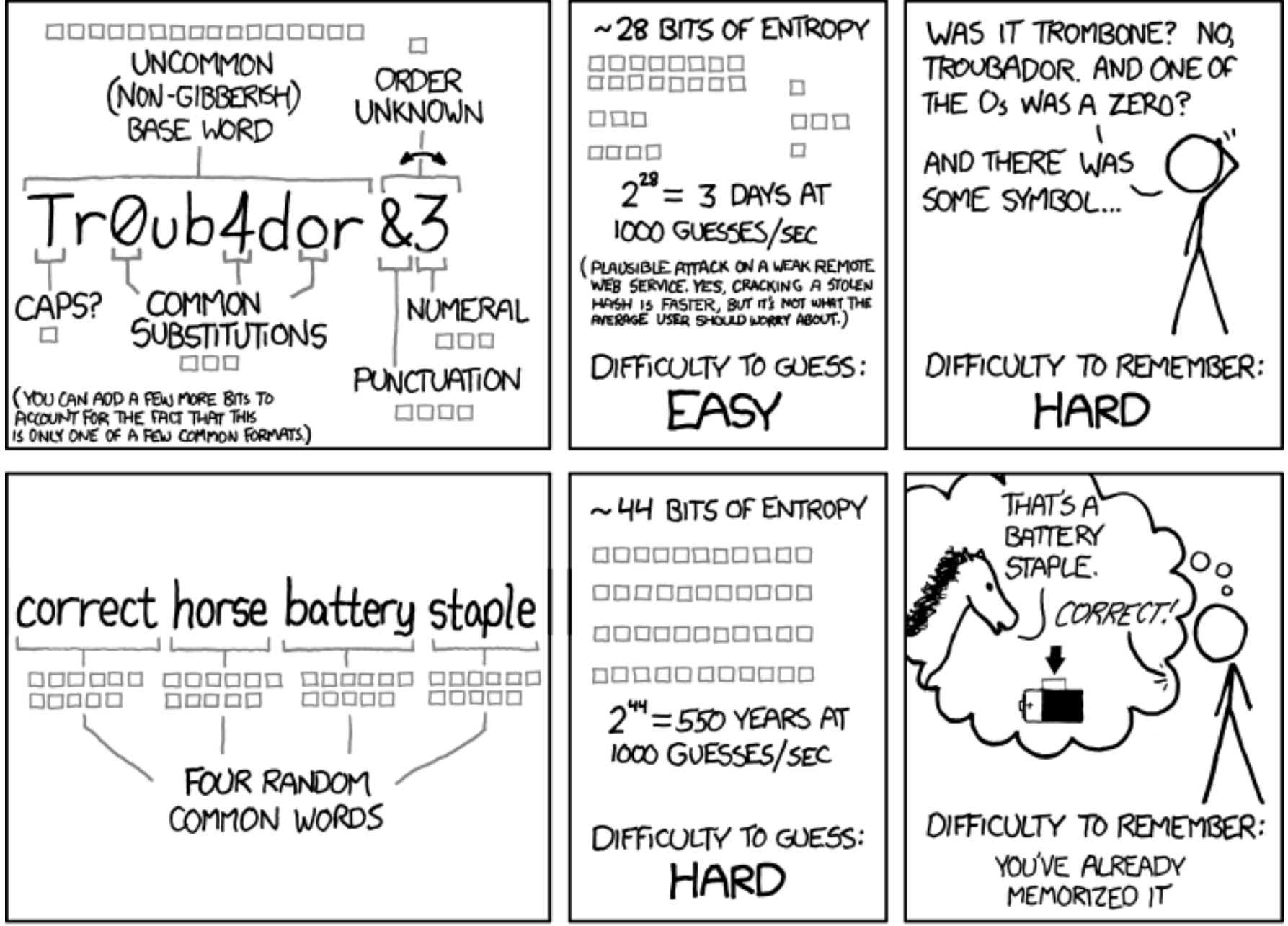
- Change frequently…
- Use Strong passwords
- Don’t reuse passwords
- Don’t base on personal information (In general)


With my ailing memory, I'm thinking
of changing my password to "incorrect"
That way, when I log in with the wrong
password, the computer will tell me..
"Your password is incorrect"

Memorable Passwords – Pass Phrase

- **Remember a sentence and use letters from that.**
- **“The first house I ever lived in was 613 Fake Street. Rent was $400 per month.”**
- **Tfh1eliw613FS.Rw$4pm.**

- How to Create a Strong Password (and Remember It)


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

From XKCD

Memorable Passwords – Random Words

- Now need at least six random words
- Not based on phrases or connected in a logical way
- Use memorization tactics (*e.g.* strategies people use to memorize random lists)

Password Group Activity

- **10 minutes discuss**
- **10 minutes report**
- **Break into groups**
- **Report:**
  - Come up with a couple of strong passwords that are relatively easy to remember. Of course you wouldn’t want to use the ones that you share.
  - Explain how you came up with the password and how you made it memorable.

Dealing with Multiple Passwords

- **Passwords for**
  - Bank
  - Phone
  - Cable
  - Facebook
  - Twitter
  - ……

From http://www.telegraph.co.uk/

Dealing with Multiple Passwords

- **Password Classes**
  - Reuse passwords for different types of accounts
  - Weak
- **Add domain info to password classes**
  - Like above, but modify password by adding domain information
  - Now weak

From http://www.telegraph.co.uk/

Dealing with Multiple Passwords

- **Password Managers**
  - Locally based
  - Cloud based

  - PC Magazine Ratings
  - Lifehacker Reviews
  - I use LastPass
    - What if hacked?

From http://www.telegraph.co.uk/

Password Storage

- If server is hacked,
  how safe is my password?

- Correct “Hash” / One Way Encryption
- Incorrect – password itself
- Salt

Authentication

- **Factors:**
  - Knowledge Factors
  - Ownership Factors
  - Inherence Factors

- **Password is a knowledge factor**

- **What if password is compromised???**

Two Factor / Multifactor Authentication

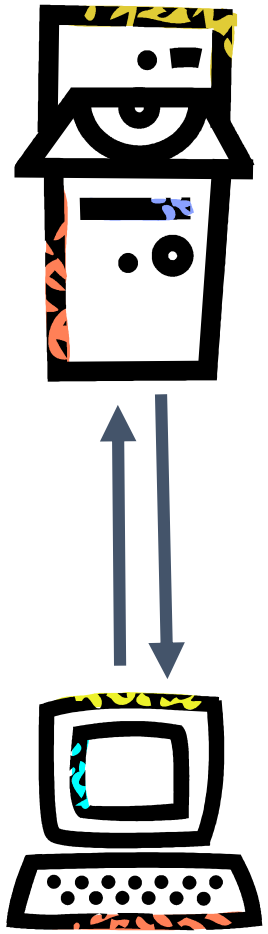
- **Use more than one factor**

- **Examples**
  - Github
  - Google Authenticator

Personal Knowledge

- Social Media
- Twitter Program Story
- Facebook Post
  - “Hey I’m not at home so come rob me!”
- Astros Hacking

Webpages



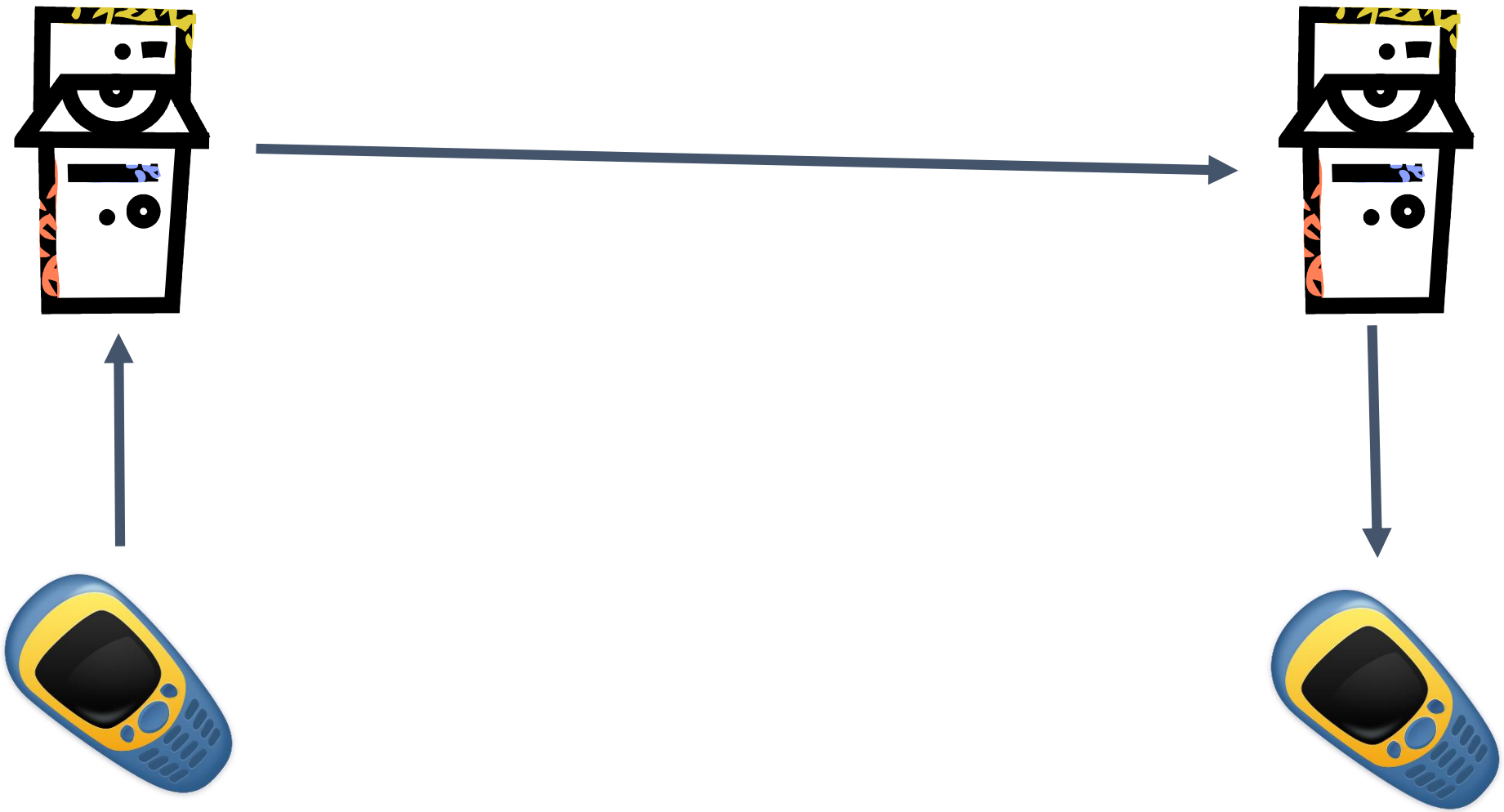
- Https://

Email

Secure Email

- **Difficult to Implement**
- **PGP**
  - Have to get both sides to coordinate
- **Secure Email Services**
  - Eg: ProtonMail

SMS



Secure Messaging

- Secure Messaging Scorecard

Other issues/questions?

Information Security Group Activity

- 10 min discuss
- 10 min report
- Break into your groups.
- Come up with at least three ways that information security can be compromised in electronic media. Keep this one general, we'll tie things to interpreting later.

Refresh: Illustrative Behavior - Interpreters

1.1 Share assignment-related information only on a confidential and "as-needed" basis (e.g., supervisors, interpreter team members, members of the educational team, hiring entities).

1.2 Manage data, invoices, records, or other situational or consumer-specific information in a manner consistent with maintaining consumer confidentiality (e.g., shredding, locked files).

CPC Group Activity – Part B

- 15 minutes discuss
- 10 minutes report
- Break into your groups.
- Refer to your notes from the first group activity.
- Come up with at least two examples of how tenants 1.1 and 1.2 can be compromised.

CPC Group Activity – Part C

- 15 minutes discuss / 10 minutes report
- Break into your groups.
- Based on examples from part B, what is a strategy for preventing at least two scenarios where tenants 1.1 and 1.2 can be compromised.

Closure

- Other CPC tenants that can be compromised by the use of technology?
- Questions?

Bibliography

- https://pixabay.com/
- https://www.eff.org/secure-messaging-scorecard
- http://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/
- http://www.rid.org/ethics/code-of-professional-conduct/
- https://en.wikipedia.org/wiki/Authentication
- http://www.telegraph.co.uk/finance/personalfinance/bank-accounts/11037201/Clever-tricks-to-remember-your-passwords.html
- http://lifehacker.com/5529133/five-best-password-managers
- http://www.bustspammers.com/phishing_links.html
- http://www.pcmag.com/article2/0,2817,2407168,00.asp
- http://www.informit.com/articles/article.aspx?p=1350956&seqNum=3 https://www.veracode.com/blog/2013/03/hacking-the-mind-how-why-social-engineering-works

Contact

- http://jmichaelmoore.net
- jmichael@cse.tamu.edu
- terp@jmichaelmoore.net