Capabilities and Confused Deputy

- Compiler acting for Alice is confused
- There has been a separation of **authority** from the **purpose** for which it is used
- With ACLs, it's more difficult to avoid the confused deputy.
- In contrast, with capabilities it's relatively easy to prevent this problem, ***since capabilities are easily delegated***, while ACLs are not.
- In a capabilities-based system, when Alice invokes the compiler, she can simply give her C-list to the compiler. The compiler then consults Alice's C-list when checking privileges before attempting to create the debug file

ACLs vs. Capabilities (3)

- **ACLs:**
  1. Good when users manage their own files
  2. Protection is data-oriented
  3. Easy to change rights to a resource
- **Capabilities:**
  1. Easy to delegate — avoid the confused deputy
  2. Easy to add/delete users
  3. More complex to implement and they have somewhat higher overhead
- *Despite their security advantage, many of the difficult issues inherent in distributed systems arise in the context of capabilities. Thus, ACLs are used in practice far more often than capabilities*

Turing Test

- This test was proposed by Alan Turing in 1950:
  1. Human asks questions to a human and a computer, without seeing either
  2. If questioner cannot distinguish human from computer, computer passes
- This is the **gold standard** in AI
- No computer can pass this today
- But some claim they are close to passing

CAPTCHA

- **CAPTCHA** (**C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part) !!!
- Also known as **HIP** == **H**uman **I**nteractive **P**roof
- It is a test that a human can pass, but a computer can't pass with a probability better than guessing.
- This could be considered as a sort of inverse Turing test.
- CAPTCHA purpose is that only humans get access (not bots/computers). So, CAPTCHA is for **access control**
- The assumptions here are that the test is generated by a computer program and graded by a computer program, yet no computer can pass the test

CAPTCHA Uses?

Today, CAPTCHAs are used in a wide variety of applications. For example:

1. Free email services — spammers like to use bots to sign up for 1000s of email accounts. CAPTCHA employed so only humans get accounts
2. Sites that do not want to be automatically indexed by search engines. CAPTCHA would force human intervention

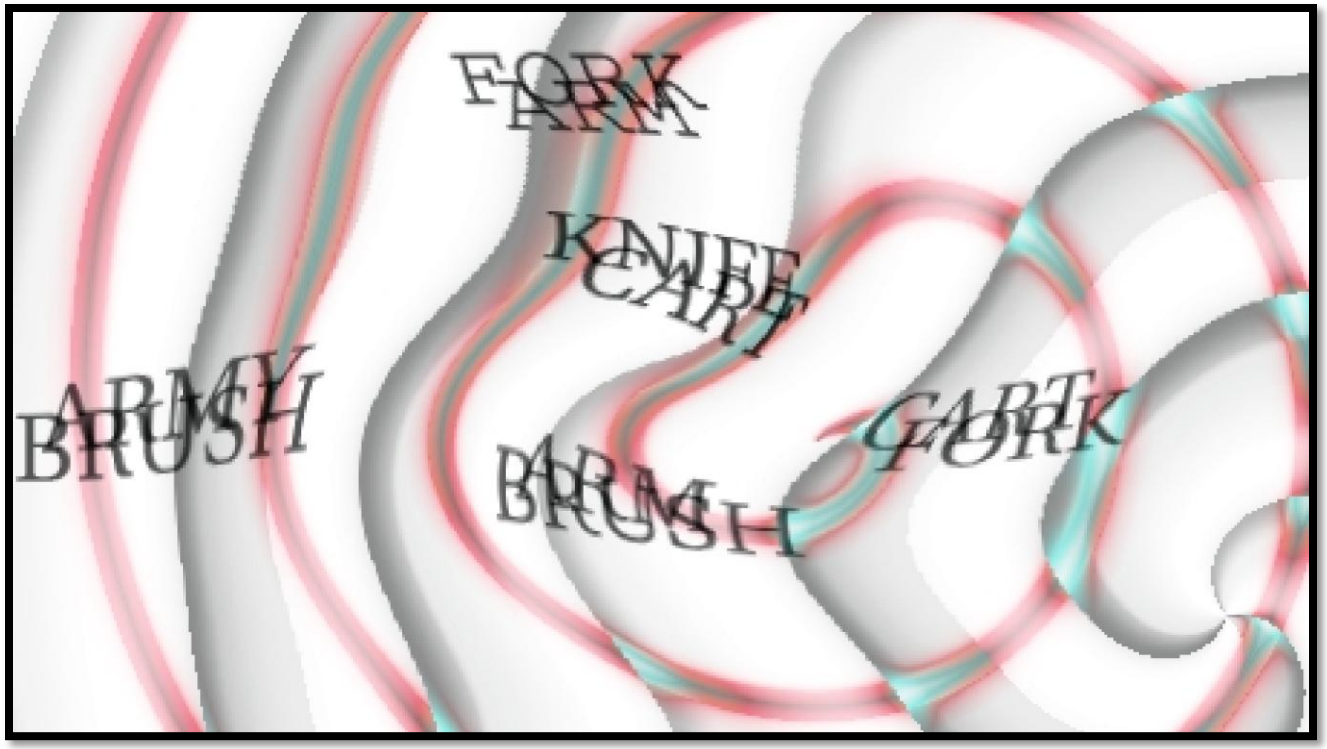
CAPTCHA: Rules of the Game

Requirements for CAPTCHA include:

1. Easy for most humans to pass
2. Difficult or impossible for machines to pass; e**ven with access to CAPTCHA software**
3. From attacker's perspective, the only unknown is a random number that is used to generate the specific CAPTCHA (Similar to Kerckhoffs' Principle)
4. Good to have different CAPTCHAs in case someone cannot pass one type. For example, many websites allow users to choose an *audio CAPTCHA* as an alternative to the usual *visual CAPTCHA*.

CAPTCHA Example 1

- In this example, a human might be asked to find three words that appear in the image.
- This is a relatively easy problem for humans and today it is also a fairly easy problem for computers to solve
- Much stronger CAPTCHAs exist



Fundamental visual CAPTCHA problems

Modern text-based CAPTCHAs are designed such that they require the simultaneous use of the following three separate abilities to correctly complete the task with any consistency:

1. ***Invariant recognition***; refers to the ability to recognize the large amount of variation in the shapes of letters. There are nearly an infinite number of versions for each character that a human brain can successfully identify. The same is not true for a computer.
2. ***Segmentation***, or the ability to separate one letter from another, is also made difficult in CAPTCHAs, as characters are crowded together with no white space in between.
3. ***Context*** is also critical. The CAPTCHA must be understood holistically to correctly identify each character. For example, in one segment of a CAPTCHA, a letter might look like an “m.” Only when the whole word is taken into context does it become clear that it is a “u” and an “n.”

CAPTCHA Example 2

- Each of these problems poses a significant challenge for a computer. The presence of all three at the same time is what makes CAPTCHAs difficult to solve
- It has been shown that computers are actually better than humans at solving all of the fundamental visual CAPTCHA problems, with one exception—the so-called ***segmentation problem***
- The segmentation problem is the problem of separating the letters from each other.
- Consequently, strong CAPTCHAs tend to look more like:

Types of CAPTCHAs

1. ***Text-based CAPTCHAs*** like previous examples. Here, we assume that attacker knows the set of possible words that could appear and he/she knows the general format of the image, as well as the types of distortions that can be applied. The only unknown for him/her is a random number that is used to select the word or words and to distort the resulting image
2. There are also ***audio (words or music) CAPTCHAs*** in which the audio is distorted in some way. The human ear is very good at removing such distortion, while automated methods are not so good
3. No text-based CAPTCHAs like ***image recognition CAPTCHAs*** which require users to identify simple objects in the images presented.

CAPTCHA's and AI

- Optical Character Recognition (OCR) is a challenging AI problem. Hardest part is the **segmentation problem.** Humans good at solving this problem
- Distorted sound also makes good CAPTCHA. Humans also good at solving this
- Hackers who break CAPTCHA have solved a hard AI problem. So, putting hacker's effort to good use!
- However, there are other ways to defeat CAPTCHAs. For example, the attackers may not play by the rules. Instead, the so-called *CAPTCHA farming* is possible, where humans are paid to solve CAPTCHAs (examples?!).

Finally . . .

- *Acknowledgment:* These lecture notes are based on the textbook by Mark Stamp and ppt slides offered by him. My sincere thanks are devoted to him and to all other people who offered the material on the web.

- Students are advised to study and solve the problems and answer the questions in Assignment-10.