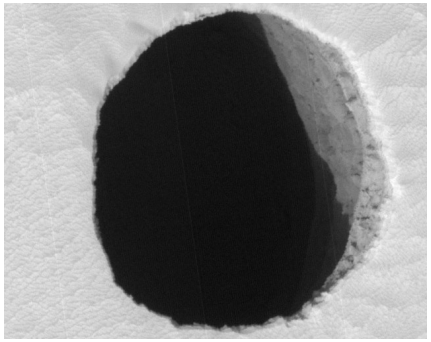
CSCD 303
Essential Computer Security
Fall 2017



Security Hole

=

People

Lecture 3

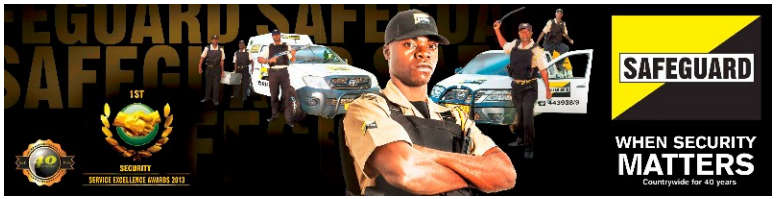
Access Control,
Authentication methods, passwords

Reading: Chapter 1, CompTIA Book,
References at end of slides

Overview

- Learning Objectives
  - Introduce Access Control
    - Identification,
    - Authentication,
    - Authorization
    - Technologies for authentication
      - Passwords, Smart Cards, Other

Access Control



- Great deal of security involves safeguarding resources or assets
  - Allowing use of resources by entities (people and systems) and
  - Preventing use of resources by entities not authorized to use the resources
  - How do we do it?
  - Physical world,

    How do you safeguard resources?
  - Digital world,

    How do you safeguard resources?

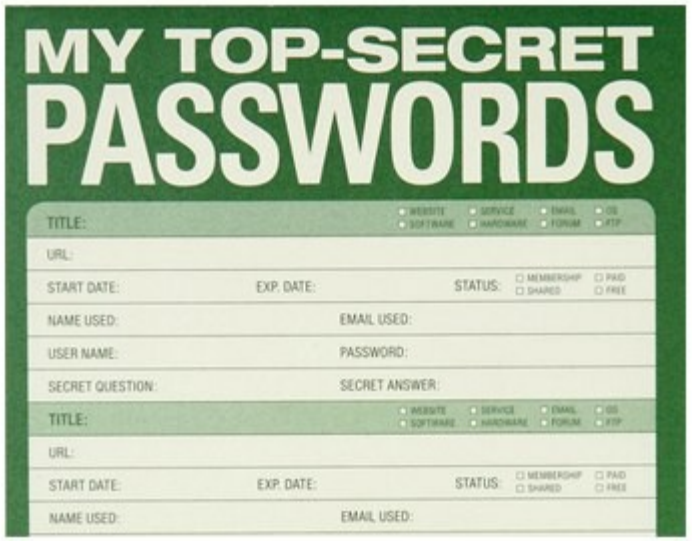
Digital World

- Identification
  - User claims identity with username or email
- Authentication
  - User proves identity, password or other technique
- Access Control
  - Authorization given based on user provided proof of identity, granted permission to use resources

Authentication Factors

- Something you know, password
- Something you have, smart card, token
- Something you are, physical
- Somewhere you are, location
- Something you do, gestures on a screen

Something you Know



Passwords

as Authentication Mechanisms

Passwords

- Fortunately or unfortunately ...
- Users must be entrusted with security of their own systems
  - Passwords still used extensively as way to authenticate people
  - Why are they still used?
  - Easy to use, know how to use them, people are familiar with them, cheap!!
  - Can be used both locally and remotely
    - On your home devices and over the Internet

Passwords

- Important to remember why passwords are important
  - Passwords are often first and sometimes only defense against intrusion

How Passwords are Used

- Authentication Process
  - User creates a password, a hash is computed and stored
    User then later enters their password, Example: catdog
  - Hash is computed, Hash(catdog) = sMxYb7$og4uxH4oHXAVwf
  - The computed hash is compared to stored hash
  - Access granted or denied … its that simple

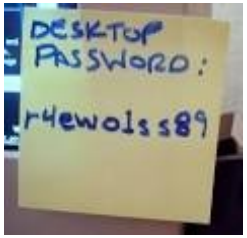
- Windows Files

  On Windows systems password hashes are stored in the SAM (Security Accounts Manager) database C:/Windows/system32/config

- Unix/Linux Files

  On Unix/Linux systems password hashes are stored in the /etc/shadow file

Password Weaknesses



- If password is sent in clear, can be intercepted
- Password is encrypted, requires encryption key

  If key is stored, can a key be compromised?

- **Also ….**
  - People choose bad passwords
  - Passwords are easily observed
  - Passwords can be sniffed by spyware or key loggers

  - And, people can be tricked … pretty easily !!!!

People Give away Passwords

http://news.bbc.co.uk/2/hi/technology/3639679.stm

- Security crumbles in the face of sweet bribes
- More than 70% of people would reveal their computer password in exchange for a bar of chocolate, according to a survey in the UK
- It also showed that 34% of respondents volunteered their password when asked without even needing to be bribed

Disadvantages of Passwords

Note: Passwords are generally pretty weak

- University of Michigan:
    - 5% of passwords were goblue
- Passwords often used in more than one place

Disadvantages of Passwords

Attacker can access the hashed password

- Can guess and test passwords offline

  "password cracking"

Lots of help

- Programs to break passwords – all these programs are distributed in Kali Linux
  - John the Ripper
  - Rainbow Crack
  - Hydra

How to Break Passwords

- Three main ways programs “crack” passwords
  1. Dictionary attack - tries thousands of words from dictionary files as possible passwords
  - Every word from dictionary is tested in a variety of modifications, cat – tac, cat1, cated
  - Encrypt words from list of English words, compare each encryption against stored encrypted version of users' passwords

How to Break Passwords

2. Brute Force Attack

- Finds passwords by checking all possible combinations of characters from the Symbol Set
  - You can make a big Brute-Force-Dictionary to implement Brute-Force attack
  - Actually, don't have to … these come with automated tools !!!

How to Break Passwords

3. Guessing Attack – Guess based on something “known”
   - blank (none)
   - words "password", "passcode", "admin" and their derivatives
   - a row of letters from the qwerty keyboard -- qwerty itself, asdf, or uiop
   - user's name or login name
   - name of their significant other, a friend, relative or pet
   - birthplace or date of birth, or a friend's, or a relative's
   - automobile license plate number, or a friend's, or a relative's
   - office number, residence number or most commonly, their mobile number

Effectiveness of Password Guessing

How well do these work?

Guessing ...

- September 2008, Yahoo e-mail account of Governor of Alaska and Vice President of the United States nominee Sarah Palin
- Accessed without authorization by someone who researched answers to two of her security questions
  - Zip code and date of birth
  - Was able to guess the third, where she met her husband!

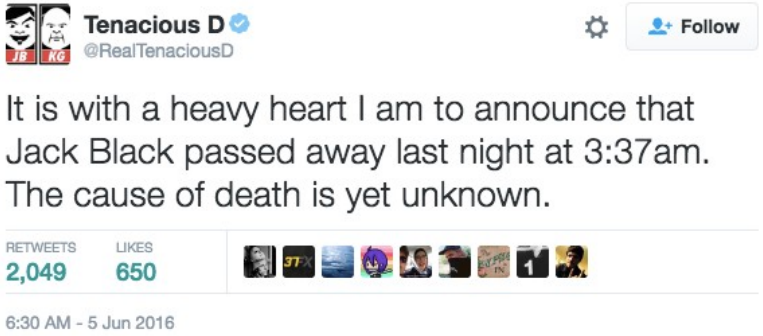
Effectiveness Password Guessing

- **Another Example**
  - Gary McKinnon, accused of perpetrating "biggest military computer hack of all time",
  - Claimed that he was able to get into military's networks by using Perl script that searched for blank passwords
  - His report suggests that there were computers on these networks with no passwords at all!
  - Story from BBC About Gary McKinnon

    http://www.bbc.com/news/uk-19946902

Modern Password Cracking

Still Alive !!!!



- More famous hacks based on passwords

  https://www.cnet.com/news/celebrity-twitter-accounts-hit-by-hackers/

  - Celebrities whose accounts were taken over included (in 2016)
    - Musician Keith Richards
    - Facebook CEO Mark Zuckerberg (Oops)
    - Actor Jack Black and others …

      Jack Black was announced dead !!!

Effectiveness of Password Cracking

PENNSTATE

Penn state CS Engineering Department

- Ran John the Ripper on CSE authentications
  - 3500 in all
- In first hour, 25% were recovered
  - About half of these due to dictionary attacks
  - But, half using other heuristics and brute force
- Over 5 days, 35% were recovered
  - Steady state recovery due to brute force

Top Password cracking software listed here

http://sectools.org/crackers.html

Password Cracking Stats - Slow

Password Length	Numeric only	Alphabetic upper-case only	Alpha-numeric Upper and lower	Alpha-numeric + Special Chars.
4	.001 sec	.046 sec	1.48 sec	8.49 sec
6	.1 sec	30.9 sec	94.7 min	21.7 hrs
7	1 sec	13.4 min	4.08 days	87 days
8	10 sec	5.80 hrs	253 days	22.9 yrs
10	16.7 min	163 days	26.6 centuries	2110 centuries
12	27.8 hrs	303 yrs	102k centuries	19.5m centuries

Note: Table based on being able to generate 10 million cracks per second

Common Password Advice

Cat or Dog – Bad
Qvmerx49z! - Good

Should be at least 8 characters

Use characters from each of the following four classes:

- English upper case letters
- English lower case letters
- Arabic numerals (0,1,2,…)
- Non-alphanumeric (special) characters such as punctuation symbols

Don’t use a proper name or any word in dictionary without misspelling it in some way

Don’t reuse password you have used before

Don’t use the same password for different types of systems

Don't Share password with anyone

Common Password Advice

Cracking statistics

General equation for password cracking

Character space ^ password length

Example: Lower case alphabet and 6 char password

26^6 = 308 million possibilities

Increase length to 10

26^{10} = 141 trillion possibilities

Modern password cracking tools,

– test > 20 billion per second

crack 10 char password in < 2 hours

Common Password Advice

Cracking statistics

Increase number of characters to 94 with

- Printable characters, upper, lower, numbers
- Special characters

Password length is 6

94^6 = 689 billion possibilities

94^{10} = 53 quintillion … will take years to crack it !!!

More Advice

1. The more complex the less secure
   - People will write them down
2. Change passwords every 45 – 90 days
3. Change default passwords

Something You Have

Smart Cards

Token

Keyfob

Smart Cards or Other tokens

Physically Real

Smart card, a plastic card with embedded technology

http://www.smartcardalliance.org/smart-cards-faq/

Combines something you have with something you know

Called **Two-Factor authentication**

Smart card chip can be either microcontroller chip or an embedded memory chip

Designed to be tamper-resistant and uses encryption to provide protection for in-memory information.

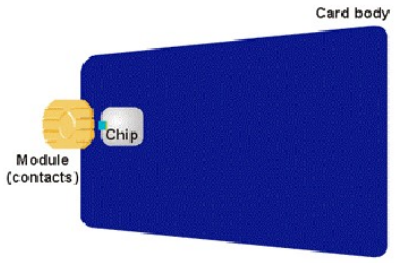
Cards with microcontroller chip have ability to perform on-card processing functions

How does a smart card work?

- All smart cards have essentially the same physical interface to the outside world, the smart card reader

- To use a smart card, an end user simply inserts it into read / write device
  where it remains for the duration
  of a session or transaction

- The user provides a PIN or password
  as they would at an ATM machine providing
  the added protection of
  Two-factor authentication
  1. Something you know
  2. Something you have



Keyfob, Dongle or Token

- A key fob is a small, programmable hardware device that provides access to a physical object.
  - Key fobs, which are also called hardware tokens, can be used to provide on-device, one-factor authentication
- In an enterprise, key fobs are used to enable two-factor and multifactor authentication
- User first enters a personal identification code (PIN) to log in to the network, followed by a pseudo-random token code generated by the key fob to gain access into the system or network
- The token code usually times out after a short period of time to prevent attackers from reusing intercepted codes
  - Considered a One-time password



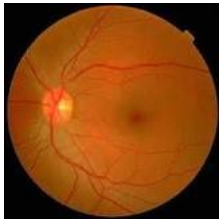
- Something You Are
- Biometric Authentication

Biometric Authentication

- Once seen mostly in spy movies (where it might be used to protect access to a top-secret military lab), biometric authentication is becoming commonplace
- Can't lose your fingerprint or handprint

  Considered to be most secure authentication methods – harder to fake biological traits
- Biometric authentication systems compare biometric data captured to stored, confirmed authentic data in a database.
  - If both samples, biometric data match, authentication is confirmed

Biometric Authentication



- **Types:**

  Retina Scans produce an image of blood vessel pattern in the light-sensitive surface lining the individual's inner eye. The pattern of cells that make up this tissue are unique to every person

  - Just like a fingerprint, there are no two retinas alike

How is it done?

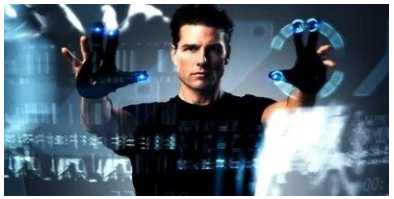
- Casts a beam of low-energy infrared light into a person's eye as they look through the scanner's eyepiece

- This beam of light traces a standardized path on the retina

The retina's intricate network of blood vessels is a physiological characteristic that remains stable throughout the life of a person.

Retinal Scans in Popular Movies

- **Retinal scans have been used in**
  - Minority Report – Everywhere to identify people …



  - Wrath of Khan, Captain Kirk gains access to top secret files with retinal scan
  - 1966 movie, Batman had a portable retinal scan in his batmobile and talked about confirming the identify of the Penguin via a retinal scan

Retinal Scans Pros and Cons

- **Pros**
  - Low false positives
  - Low false negatives
  - Highly reliable for distinguishing people
  - Speedy
- **Cons**
  - Not user friendly, invasive process
  - High equipment costs
  - Eye Disease can affect outcome
  -

Biometric Authentication

Types:

Iris Recognition is used to identify

individuals based on unique patterns within the ring-shaped region surrounding pupil whose complex random patterns are unique

How does it work?

- People have their eyes digitally photographed with both ordinary light and invisible infrared
- In iris recognition, infrared helps to show up unique features of darkly colored eyes that do not stand out clearly in ordinary light
- Identifies around 240 unique features which are turned into a simple, 512-digit number called an IrisCode® that is stored, alongside your name and other details, in a computer database

Iris Scans Pros and Cons

- **Pros**
  - Low false positives
  - Low false negatives
  - Highly reliable for distinguishing people
  - Speedy
  - Can be performed some distance from eye
- **Cons**
  - High equipment costs
  - Privacy concerns, track people at a distance

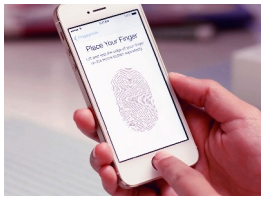
Biometric Authentication

- Types of biometric authentication technologies:

  Fingerscanning, works with details in pattern of raised areas and branches in a human finger image

  - Fingerprints are unique (even among identical twins), impossible to guess, and difficult to fake without significant effort … can be done ...
  - Modern fingerprint authentication uses fingerprint to create an encrypted key, which is sent for server authentication

Fingerprint Exploits



- In 2013, Germany's Chaos Computer Club says it has cracked protection around Apple's fingerprint sensor on its new iPhone 5S, just two days after the device went on sale worldwide.
- In a post on their site, the group says that their biometric hacking team took a fingerprint of the user, photographed from a glass surface, and then created a "fake fingerprint" which could be put onto a thin film and used with a real finger to unlock the phone
- "This demonstrates – again – that fingerprint biometrics is unsuitable as access control method and should be avoided," said the Chaos Club's blogpost author, "Starbug". "In reality, Apple's sensor has just a higher resolution compared to the sensors so far. So we only needed to ramp up the resolution of our fake. “

https://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked

Biometric Authentication

- Types of biometric authentication technologies:

  Facial Recognition systems work with numeric codes called faceprints, which identify 80 nodal points on a human face

  - Facial recognition analyzes the characteristics of a person's face images input through a digital video camera.
  - It measures overall facial structure, including distances between eyes, nose, mouth, and jaw edges
  - These measurements are retained in a database and used as a comparison when a user stands before the camera.

Biometric Authentication

- Types of biometric authentication technologies:

  Voice Identification systems rely on characteristics created by the shape of the speaker's mouth and throat, rather than more variable conditions.

    - During enrollment for a voice authentication system, a user's voice is recorded, creating what is called a voiceprint for comparison with samples taken for user identification

Summary

- Passwords have long been used as authentication methods
- Continue to be used in spite of problems
  - Cheap, familiar, embedded into modern operating systems and most devices
- Ways to make them more secure, length, composition and longevity
- Smart cards are ubiquitous for retail and banking, tokens, keyfobs used for one-time passwords
- Biometric methods becoming more popular as readers become more readily available
- Strongest method, harder to duplicate or fake

References and Reading Material

Smart Cards

https://en.wikipedia.org/wiki/Smart_card

Iris Scans

http://www.explainthatstuff.com/how-iris-scans-work.html

Blog about Retinal Scan

http://hicab-blog.blogspot.com/p/introduction-human-retina-is-thin.html

Retinal Scan

http://www.biometricupdate.com/201307/explainer-retinal-scan-technology

Fingerprint Technology

https://www.imore.com/how-touch-id-works

Key fob

http://searchsecurity.techtarget.com/definition/key-fob

Security Tokens

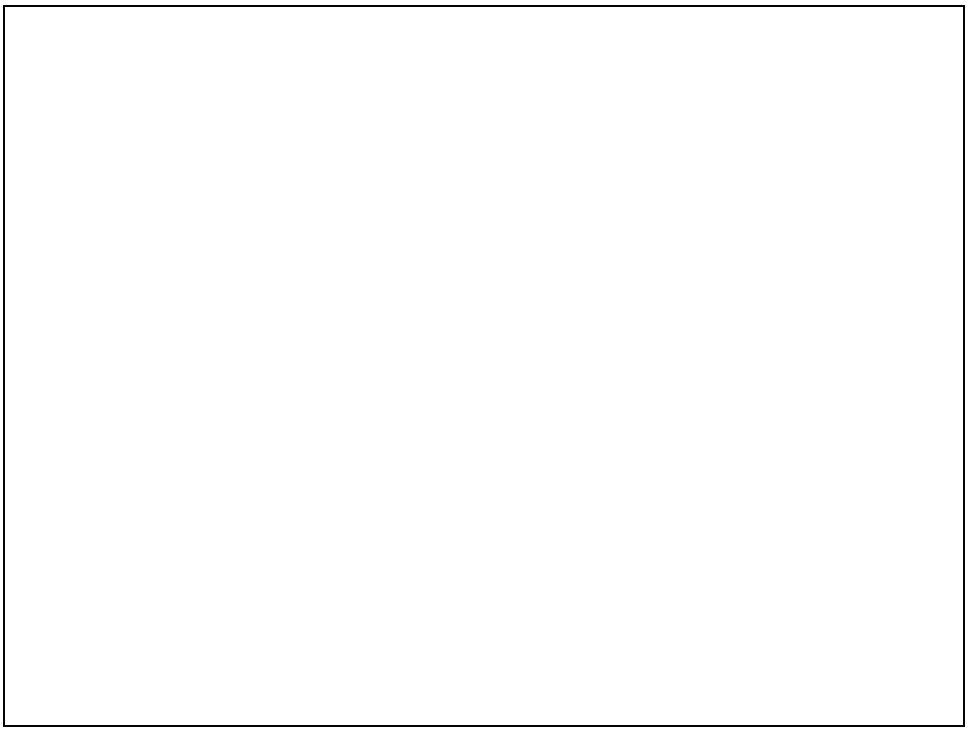
http://www.explainthatstuff.com/how-security-tokens-work.html

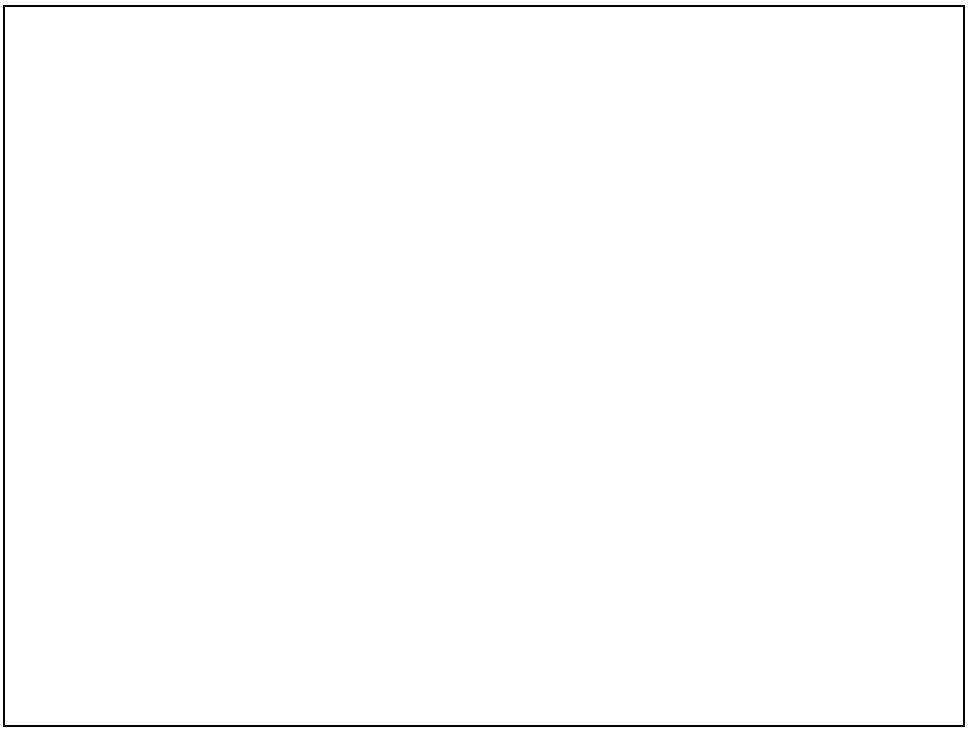
Creating a password

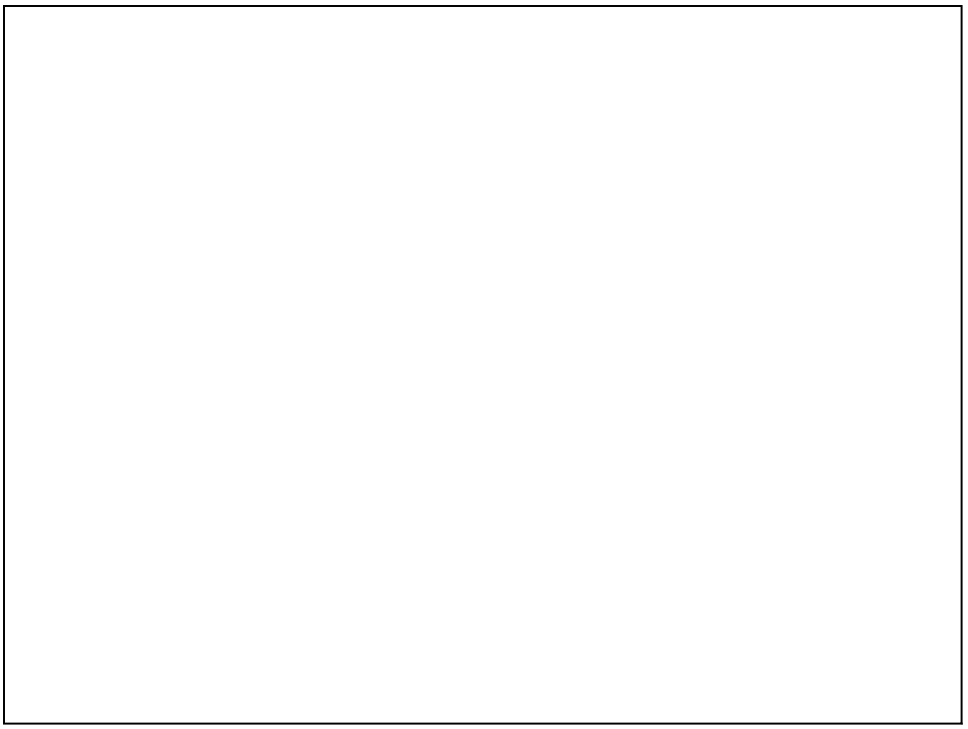
cabbage
Sorry, the password must be more than 8 characters.
boiled cabbage
Sorry, the password must contain 1 numerical character.
1 boiled cabbage
Sorry, the password cannot have blank spaces.
50fuckingboiledcabbages
Sorry, the password must contain at least one upper case character.
50FUCKINGboiledcabbages
Sorry, the password cannot use more than one upper case character consecutively.
50FuckingBoiledCabbagesShovedUpYourArse,IfYouDo
n'tGiveMeAccessImmediately
Sorry, the password cannot contain punctuation.
NowIAmGettingReallyPissedOff50FuckingBoiledCabbag
esShovedUpYourArseIfYou
DontGiveMeAccessImmediately

Sorry, that password is already in use!

The End





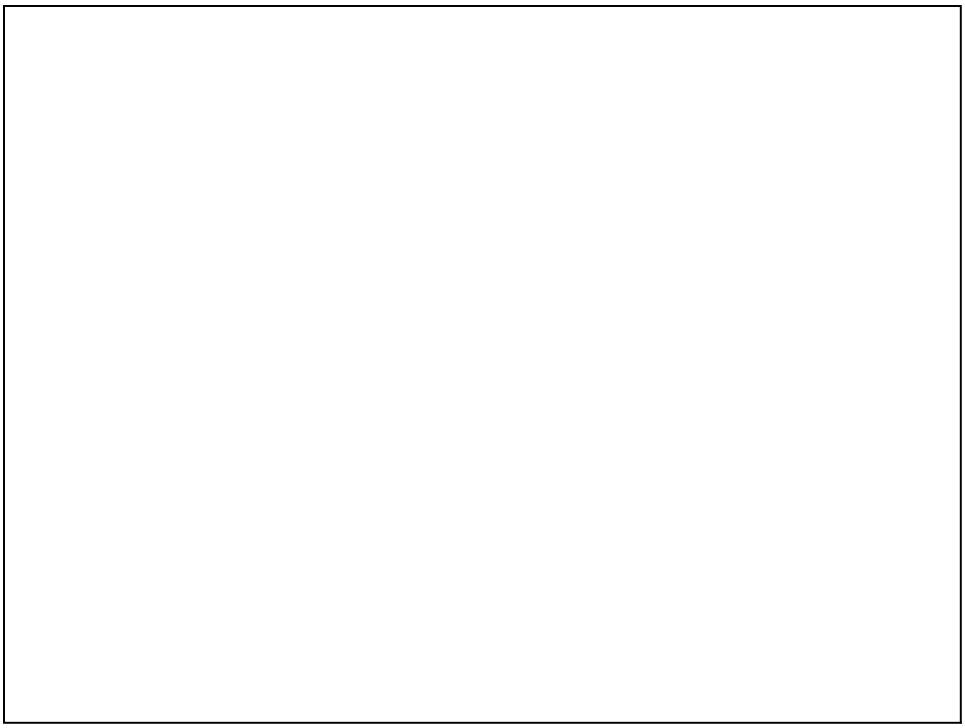


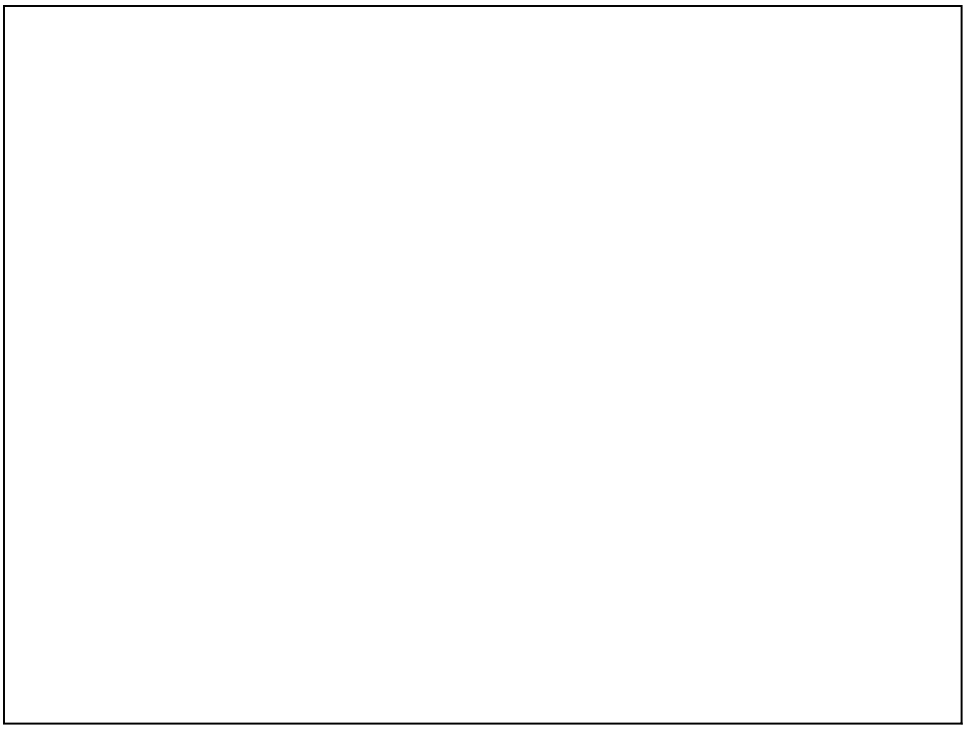
Digital World

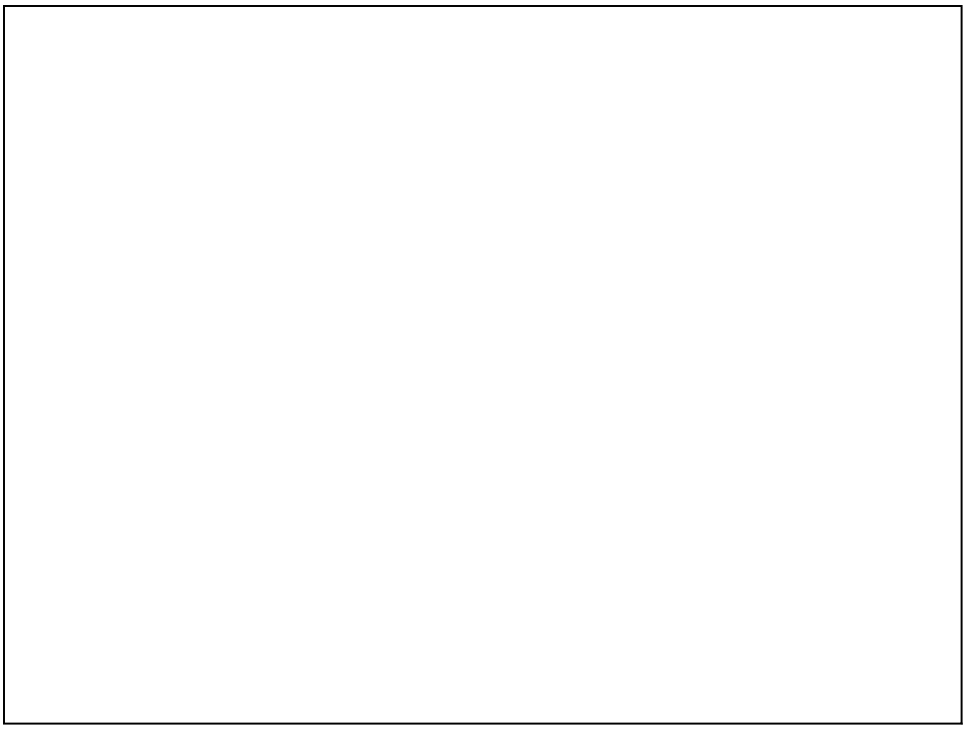
- Identification
  - User claims identity with username or email
- Authentication
  - User proves identity, password or other technique
- Access Control
  - Authorization given based on user provided proof of identity, granted permission to use resources

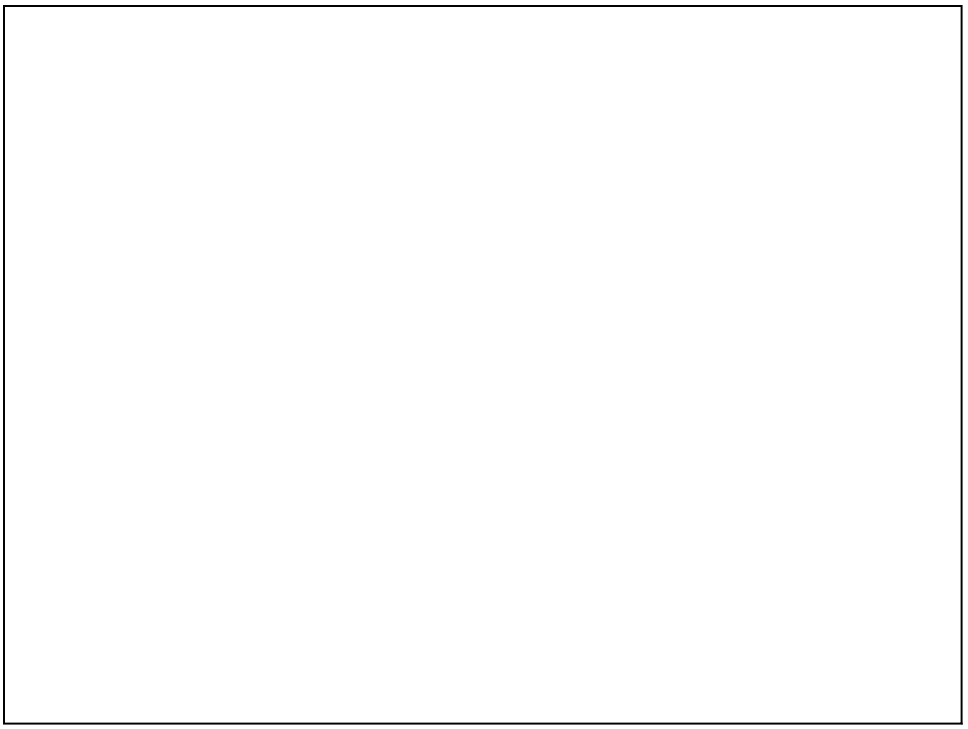
Authentication Factors

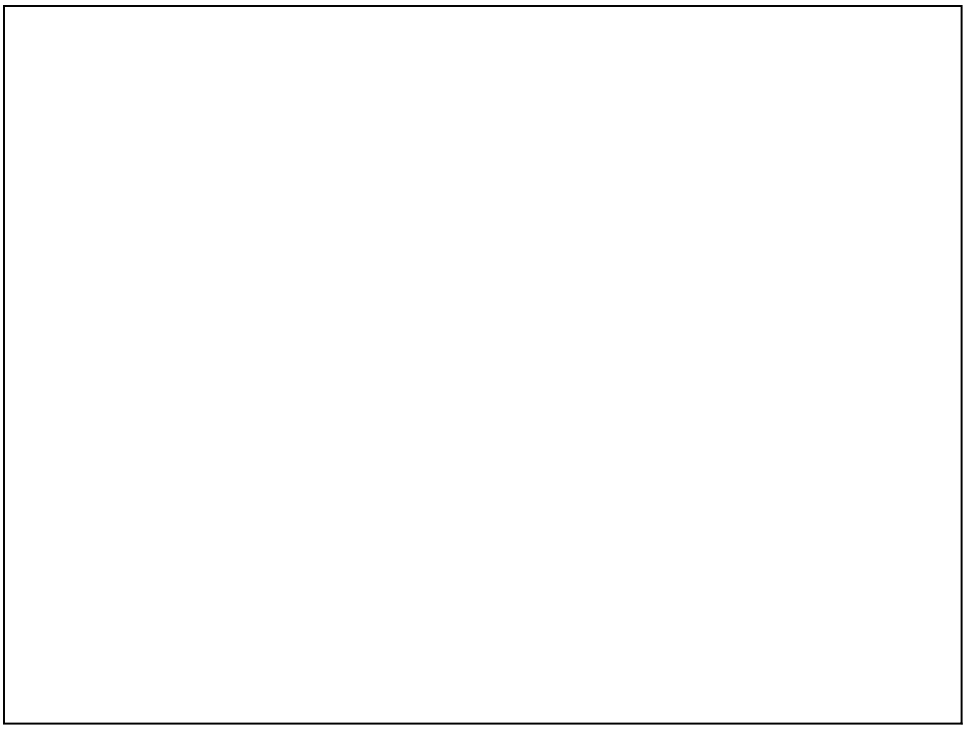
- Something you know, password
- Something you have, smart card, token
- Something you are, physical
- Somewhere you are, location
- Something you do, gestures on a screen







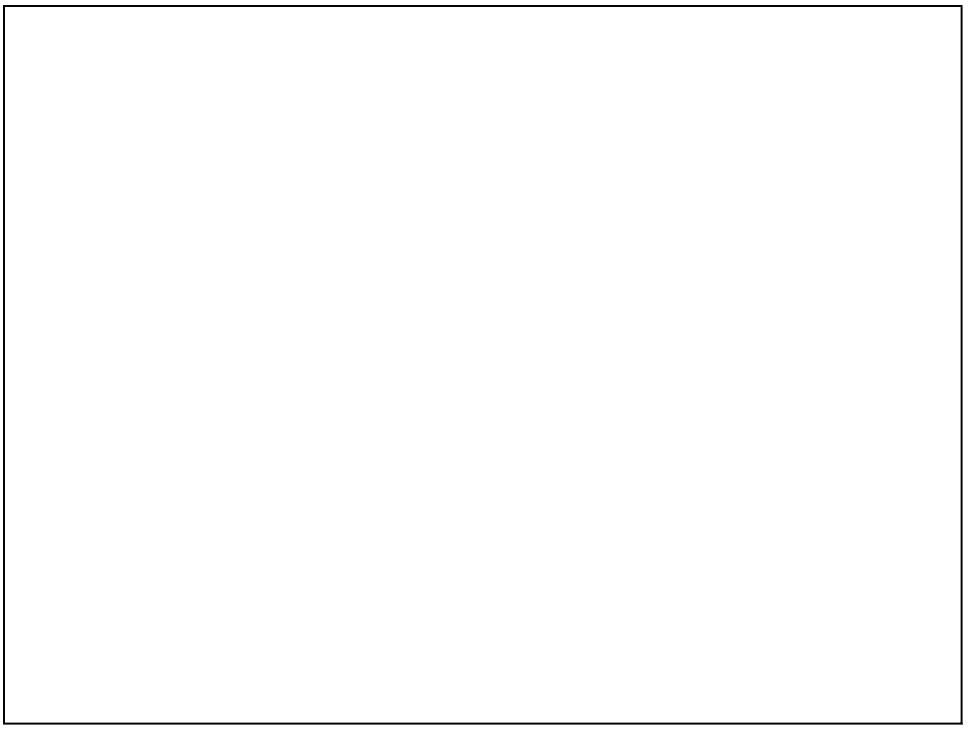


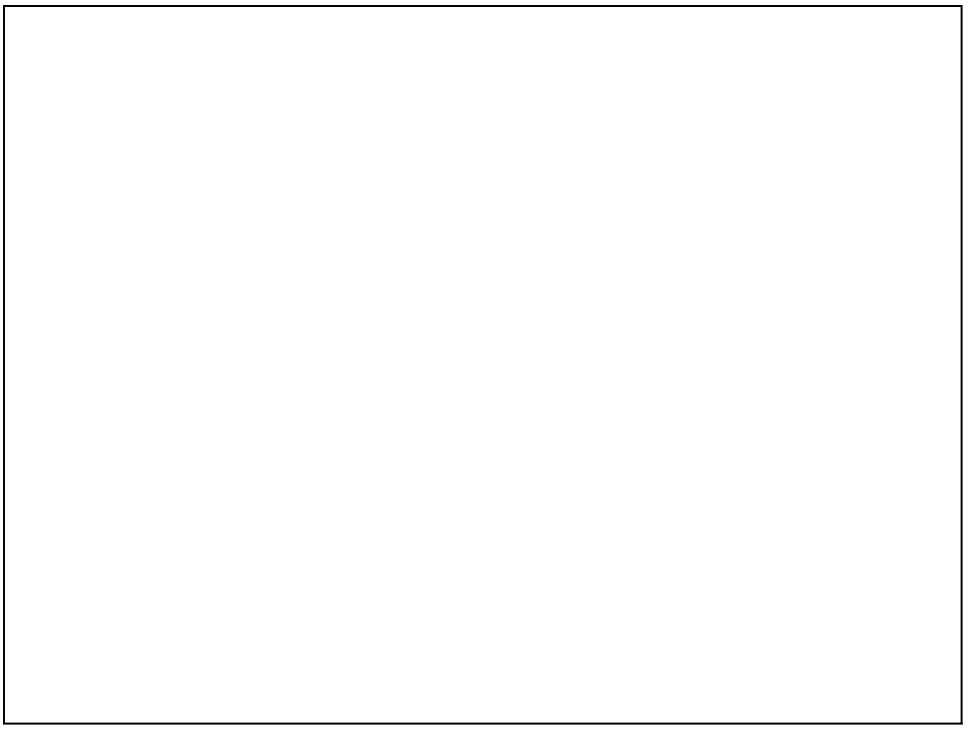


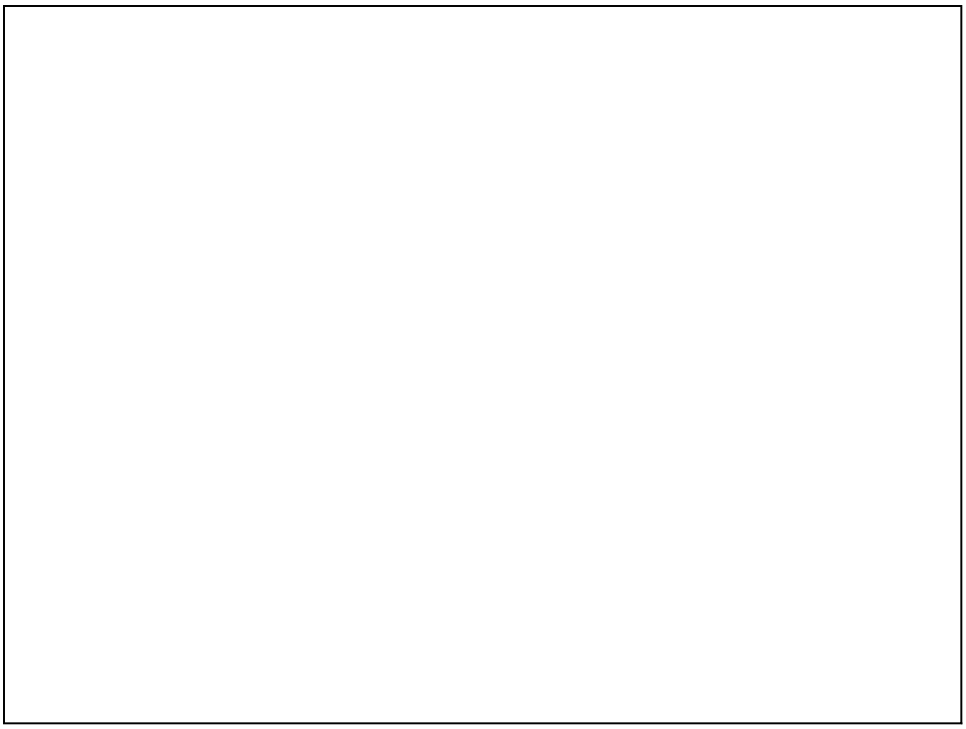
People Give away Passwords

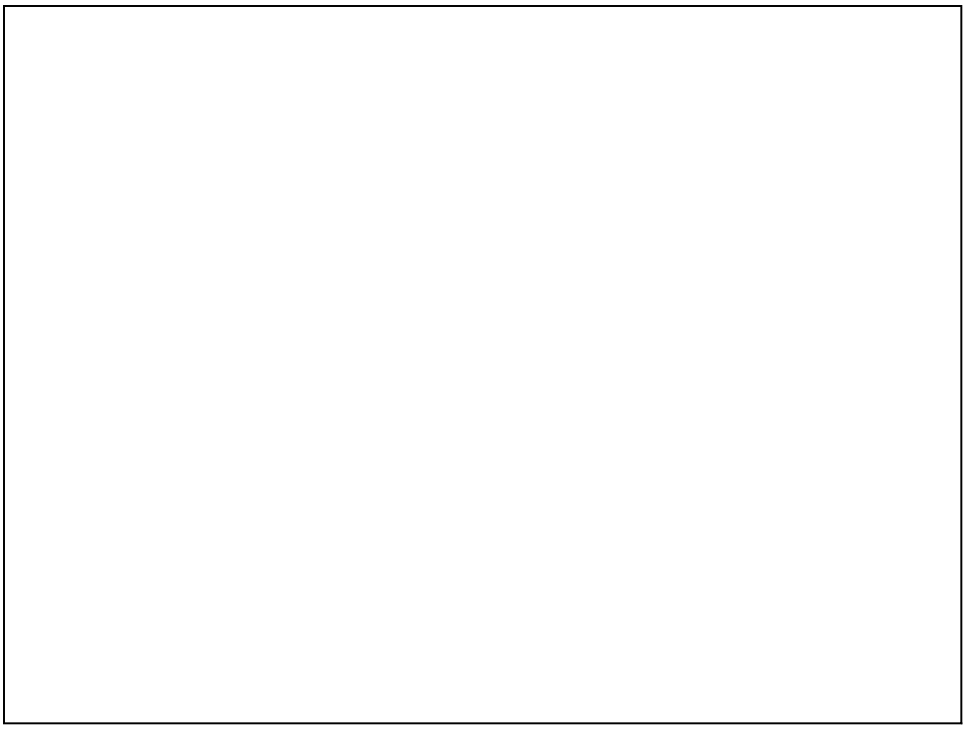
http://news.bbc.co.uk/2/hi/technology/3639679.stm

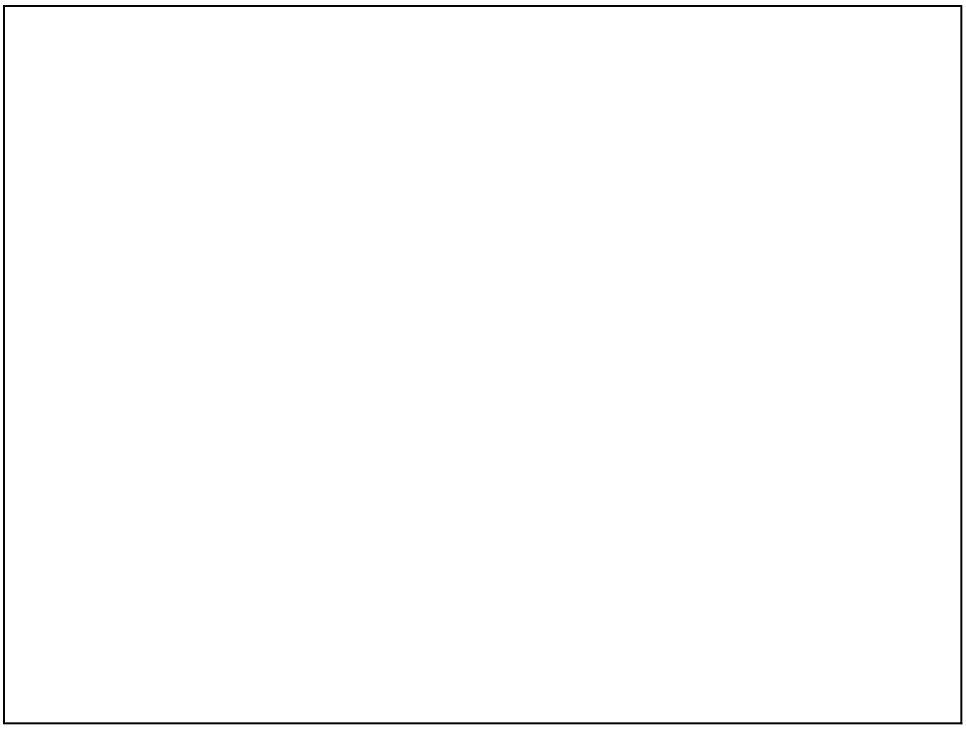
- Security crumbles in the face of sweet bribes
- More than 70% of people would reveal their computer password in exchange for a bar of chocolate, according to a survey in the UK
- It also showed that 34% of respondents volunteered their password when asked without even needing to be bribed

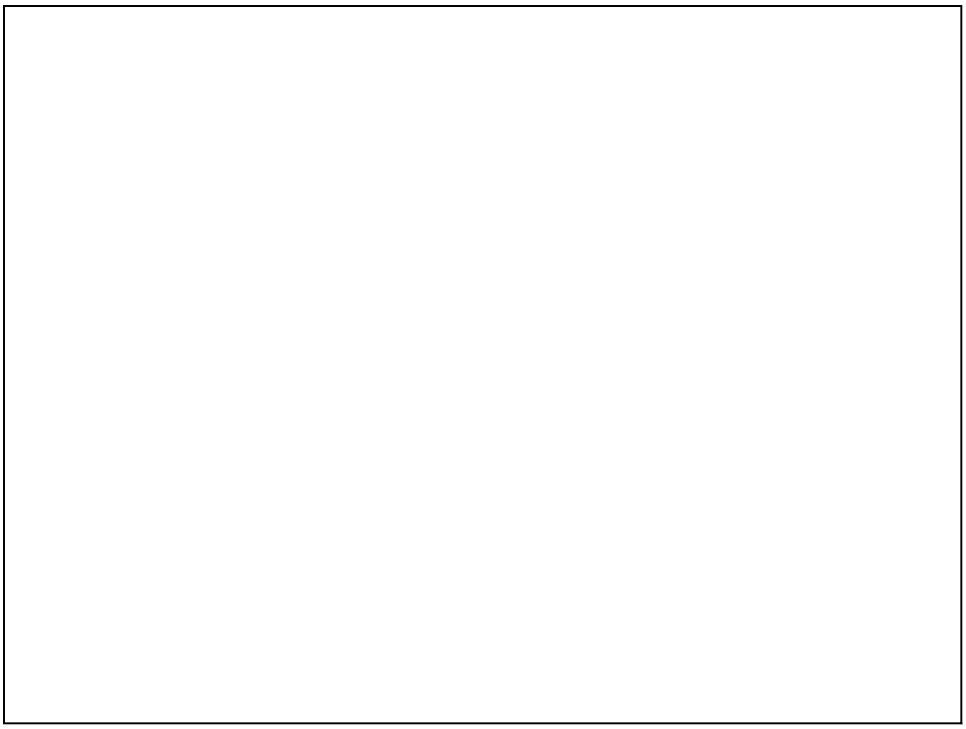


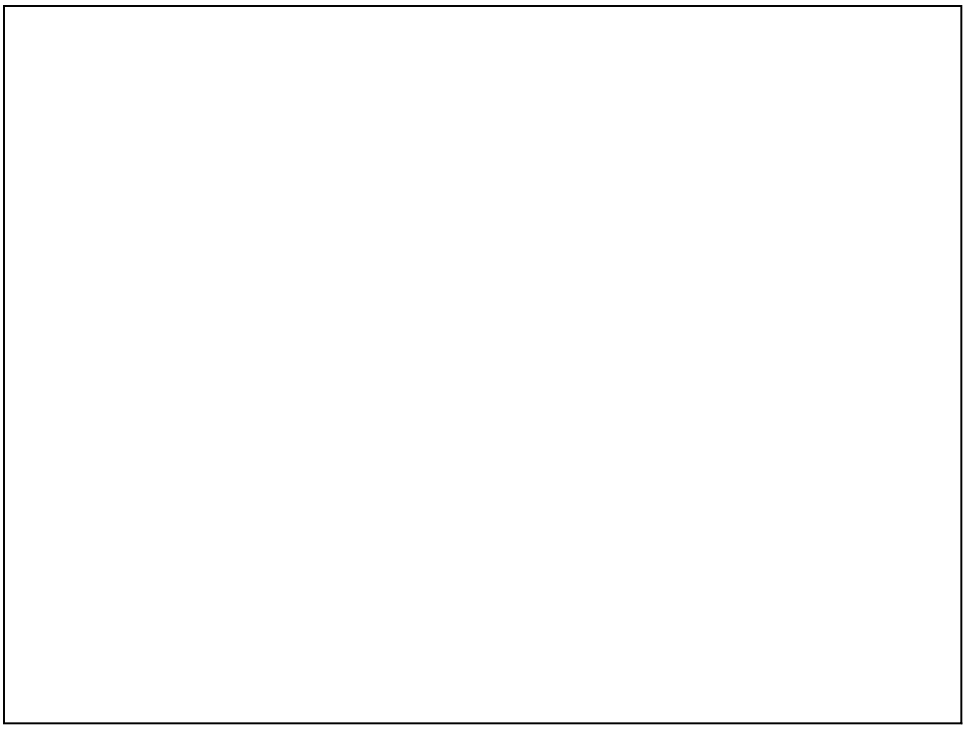












Modern Password Cracking

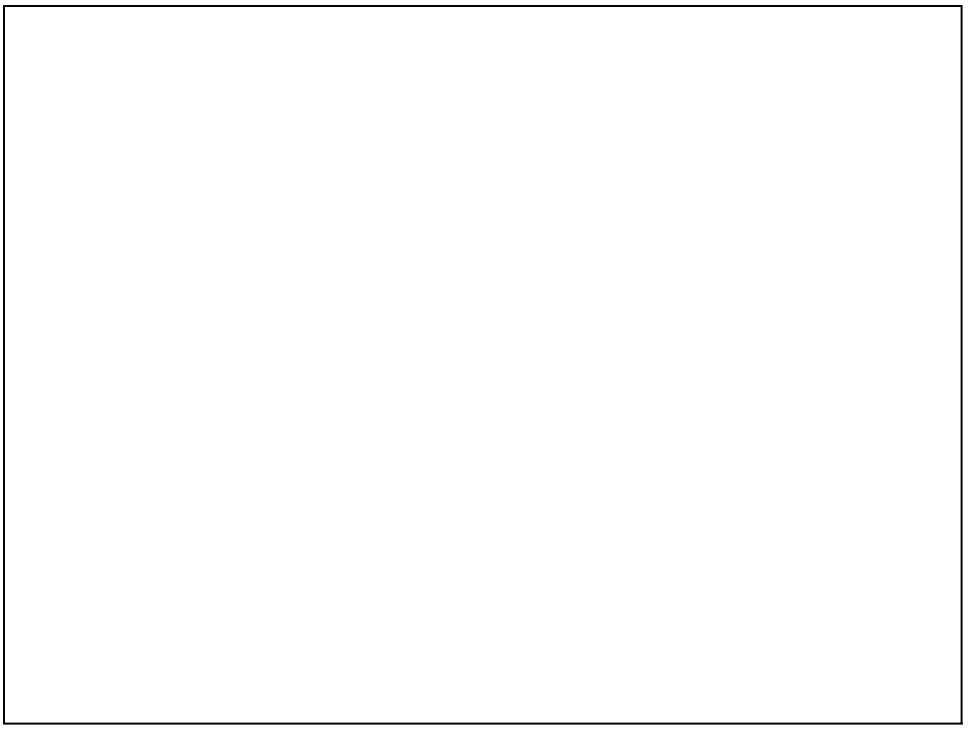
Still Alive !!!!

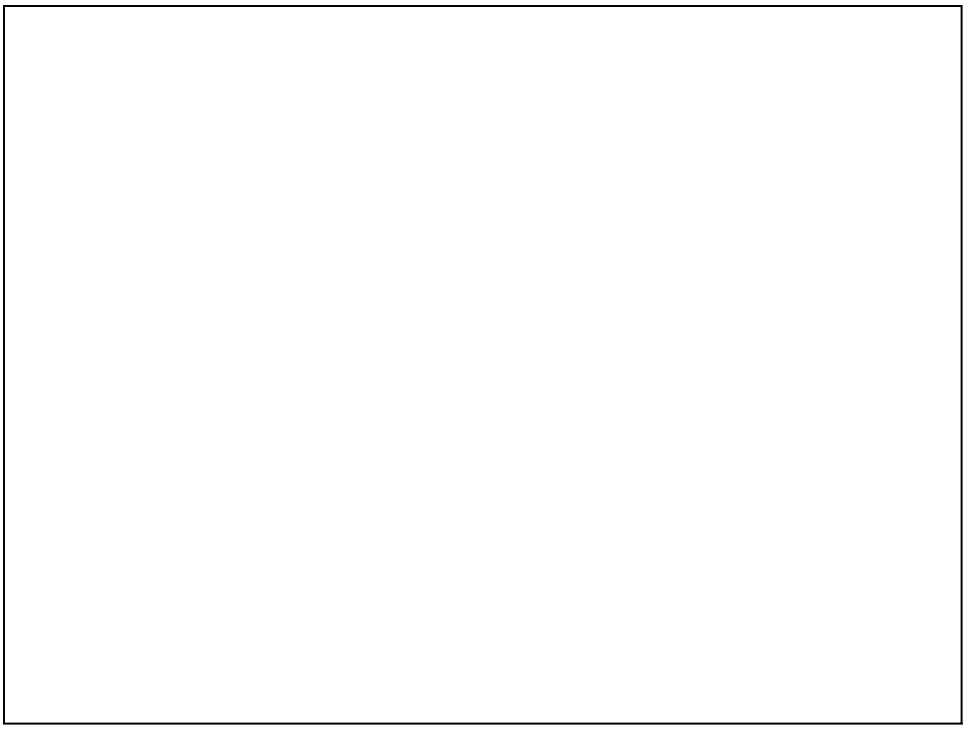
- More famous hacks based on passwords

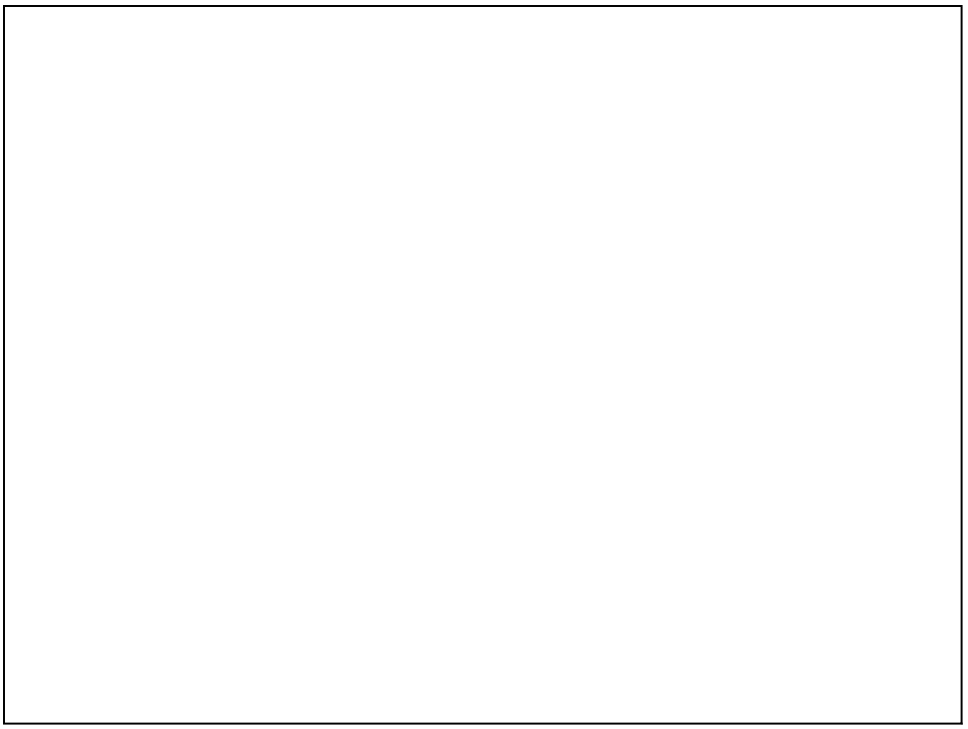
  https://www.cnet.com/news/celebrity-twitter-accounts-hit-by-hackers/

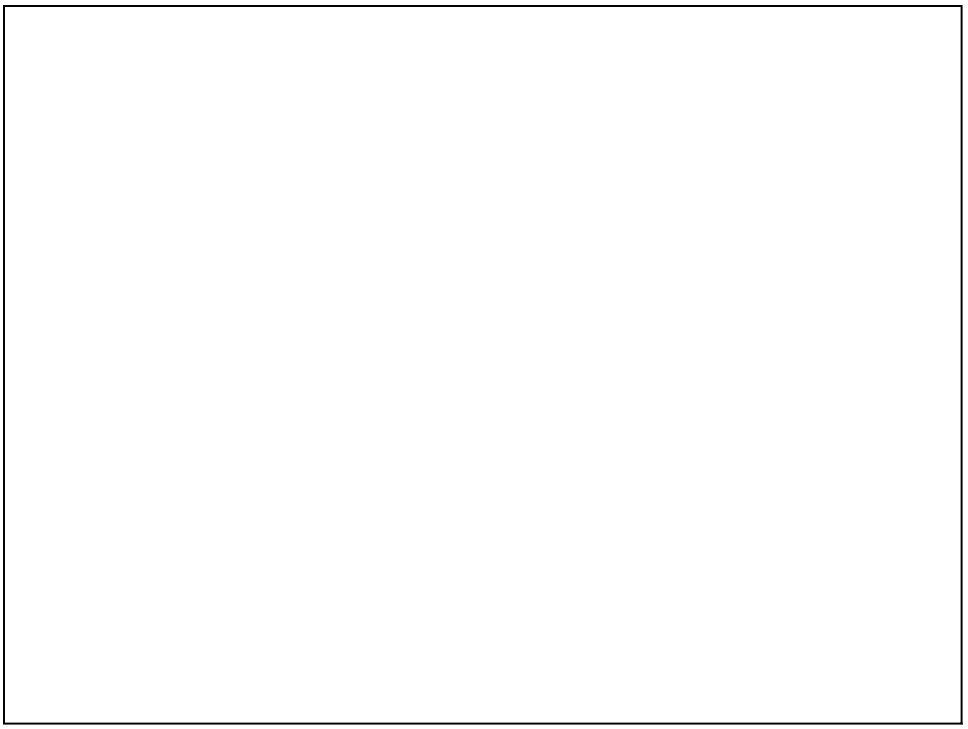
  - Celebrities whose accounts were taken over included (in 2016)
    - Musician Keith Richards
    - Facebook CEO Mark Zuckerberg (Oops)
    - Actor Jack Black and others …

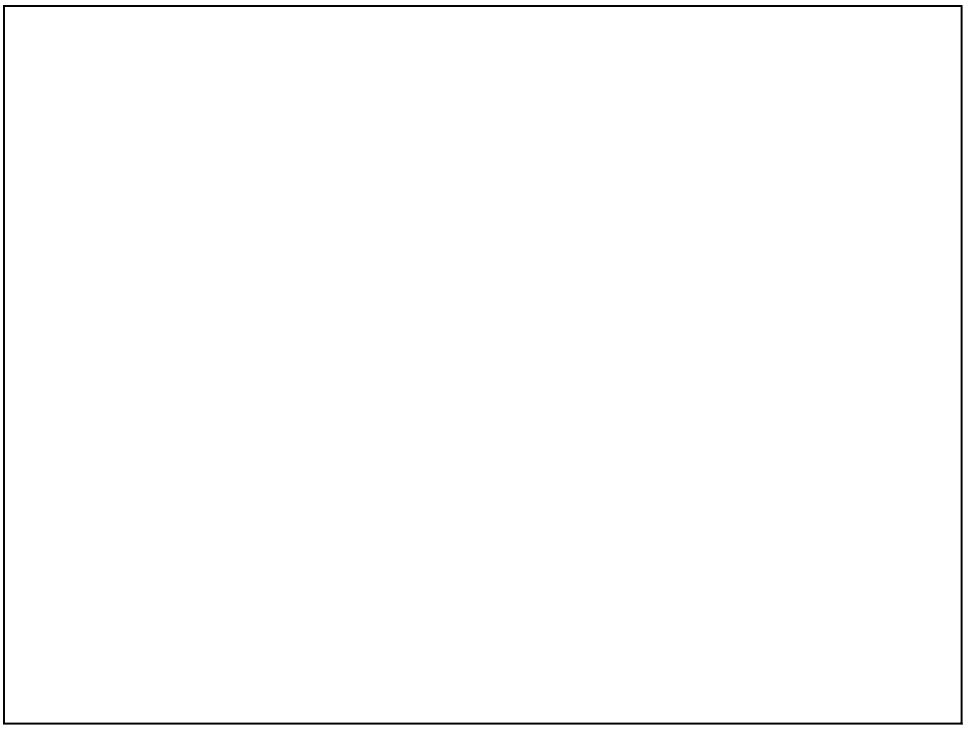
      Jack Black was announced dead !!!











Something You Have

Smart Cards

Token

Keyfob

Smart Cards or Other tokens

Physically Real

Smart card, a plastic card with embedded technology

http://www.smartcardalliance.org/smart-cards-faq/

Combines something you have with something you know

Called **Two-Factor authentication**

Smart card chip can be either microcontroller chip or an embedded memory chip

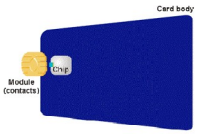
Designed to be tamper-resistant and uses encryption to provide protection for in-memory information.

Cards with microcontroller chip have ability to perform on-card processing functions

How does a smart card work?

- All smart cards have essentially the same physical interface to the outside world, the smart card reader
- To use a smart card, an end user simply inserts it into read / write device
  where it remains for the duration
  of a session or transaction

- The user provides a PIN or password
  as they would at an ATM machine providing
  the added protection of
  Two-factor authentication
  1. Something you know
  2. Something you have



Keyfob, Dongle or Token

- A key fob is a small, programmable hardware device that provides access to a physical object.
  - Key fobs, which are also called hardware tokens, can be used to provide on-device, one-factor authentication
- In an enterprise, key fobs are used to enable two-factor and multifactor authentication
- User first enters a personal identification code (PIN) to log in to the network, followed by a pseudo-random token code generated by the key fob to gain access into the system or network
- The token code usually times out after a short period of time to prevent attackers from reusing intercepted codes
  - Considered a One-time password



- Something You Are
- Biometric Authentication

Biometric Authentication

- Once seen mostly in spy movies (where it might be used to protect access to a top-secret military lab), biometric authentication is becoming commonplace
- Can't lose your fingerprint or handprint

  Considered to be most secure authentication methods – harder to fake biological traits
- Biometric authentication systems compare biometric data captured to stored, confirmed authentic data in a database.
  - If both samples, biometric data match, authentication is confirmed

Biometric Authentication

- **Types:**

  Retina Scans produce an image of blood vessel pattern in the light-sensitive surface lining the individual's inner eye. The pattern of cells that make up this tissue are unique to every person

  - Just like a fingerprint, there are no two retinas alike

How is it done?

- Casts a beam of low-energy infrared light into a person's eye as they look through the scanner's eyepiece
- This beam of light traces a standardized path on the retina

The retina's intricate network of blood vessels is a physiological characteristic that remains stable throughout the life of a person.

Retinal Scans in Popular Movies

- **Retinal scans have been used in**
  - Minority Report – Everywhere to identify people …

  - Wrath of Khan, Captain Kirk gains access to top secret files with retinal scan
  - 1966 movie, Batman had a portable retinal scan in his batmobile and talked about confirming the identify of the Penguin via a retinal scan

Retinal Scans Pros and Cons

- **Pros**
  - Low false positives
  - Low false negatives
  - Highly reliable for distinguishing people
  - Speedy
- **Cons**
  - Not user friendly, invasive process
  - High equipment costs
  - Eye Disease can affect outcome
  -

Biometric Authentication

Types:

Iris Recognition is used to identify individuals based on unique patterns within the ring-shaped region surrounding pupil whose complex random patterns are unique

How does it work?

- People have their eyes digitally photographed with both ordinary light and invisible infrared
- In iris recognition, infrared helps to show up unique features of darkly colored eyes that do not stand out clearly in ordinary light
- Identifies around 240 unique features which are turned into a simple, 512-digit number called an IrisCode® that is stored, alongside your name and other details, in a computer database

Iris Scans Pros and Cons

- **Pros**
  - Low false positives
  - Low false negatives
  - Highly reliable for distinguishing people
  - Speedy
  - Can be performed some distance from eye
- **Cons**
  - High equipment costs
  - Privacy concerns, track people at a distance

Biometric Authentication

- Types of biometric authentication technologies:

  Fingerscanning, works with details in pattern of raised areas and branches in a human finger image

  - Fingerprints are unique (even among identical twins), impossible to guess, and difficult to fake without significant effort … can be done ...
  - Modern fingerprint authentication uses fingerprint to create an encrypted key, which is sent for server authentication

Fingerprint Exploits

- In 2013, Germany's Chaos Computer Club says it has cracked protection around Apple's fingerprint sensor on its new iPhone 5S, just two days after the device went on sale worldwide.
- In a post on their site, the group says that their biometric hacking team took a fingerprint of the user, photographed from a glass surface, and then created a "fake fingerprint" which could be put onto a thin film and used with a real finger to unlock the phone
- "This demonstrates – again – that fingerprint biometrics is unsuitable as access control method and should be avoided," said the Chaos Club's blogpost author, "Starbug". "In reality, Apple's sensor has just a higher resolution compared to the sensors so far. So we only needed to ramp up the resolution of our fake. “

https://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked

Biometric Authentication

- Types of biometric authentication technologies:

  Facial Recognition systems work with numeric codes called faceprints, which identify 80 nodal points on a human face

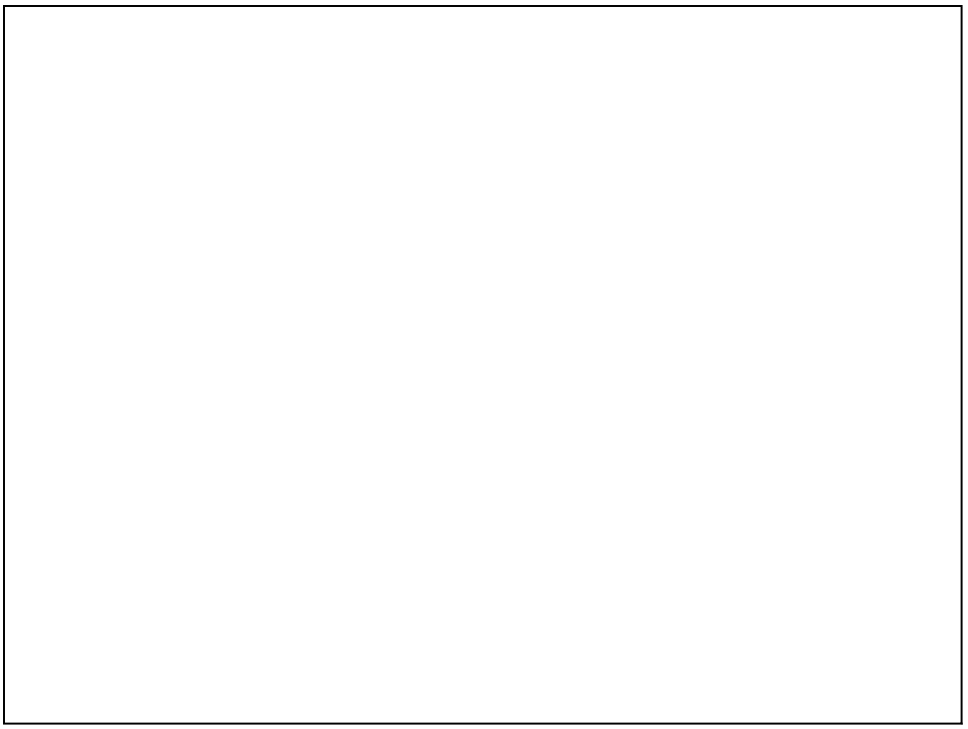
  - Facial recognition analyzes the characteristics of a person's face images input through a digital video camera.
  - It measures overall facial structure, including distances between eyes, nose, mouth, and jaw edges
  - These measurements are retained in a database and used as a comparison when a user stands before the camera.

Biometric Authentication

- Types of biometric authentication technologies:

  Voice Identification systems rely on characteristics created by the shape of the speaker's mouth and throat, rather than more variable conditions.

    - During enrollment for a voice authentication system, a user's voice is recorded, creating what is called a voiceprint for comparison with samples taken for user identification



References and Reading Material

Smart Cards

https://en.wikipedia.org/wiki/Smart_card

Iris Scans

http://www.explainthatstuff.com/how-iris-scans-work.html

Blog about Retinal Scan

http://hicab-blog.blogspot.com/p/introduction-human-retina-is-thin.html

Retinal Scan

http://www.biometricupdate.com/201307/explainer-retinal-scan-technology

Fingerprint Technology

https://www.imore.com/how-touch-id-works

Key fob

http://searchsecurity.techtarget.com/definition/key-fob

Security Tokens

http://www.explainthatstuff.com/how-security-tokens-work.html