System Security, part 1

ComS 252 — Iowa State University

Andrew Miner and Barry Britt

Disclaimer

- I am not a security expert
- This class cannot make you a security expert
  - Two lectures are not nearly enough
  - The prereqs for this class are not enough

Disclaimer

- I am not a security expert
- This class cannot make you a security expert
  - Two lectures are not nearly enough
  - The prereqs for this class are not enough

- I will teach you
  - What you are up against (i.e., why this is hard)
  - General principles to make your system safer
  - Utilities that can help you

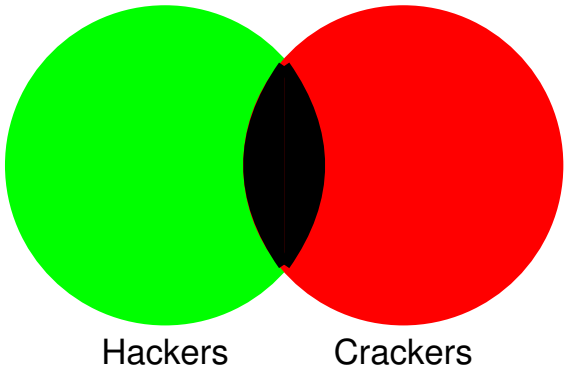
Some Terminology

hacker : someone who knows a lot about systems

- In particular, how they work
- Usually are programmers

cracker : someone who wants to crack a system

- I.e., break into a system
- Usually with malicious intent



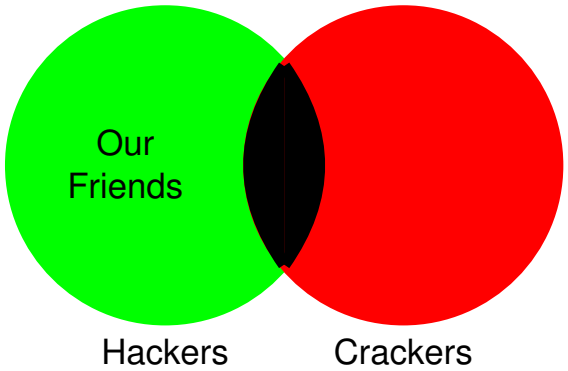
Some Terminology

hacker : someone who knows a lot about systems

- In particular, how they work
- Usually are programmers

cracker : someone who wants to crack a system

- I.e., break into a system
- Usually with malicious intent



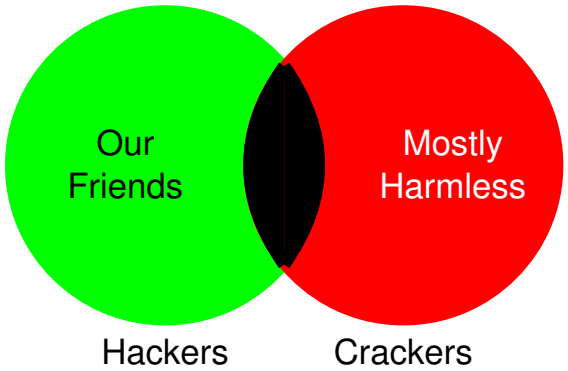
Some Terminology

hacker : someone who knows a lot about systems

- In particular, how they work
- Usually are programmers

cracker : someone who wants to crack a system

- I.e., break into a system
- Usually with malicious intent



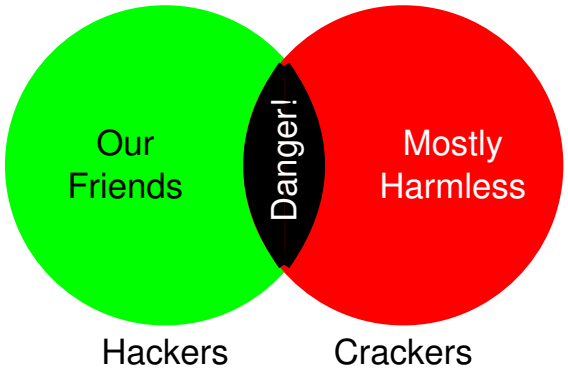
Some Terminology

hacker : someone who knows a lot about systems

- In particular, how they work
- Usually are programmers

cracker : someone who wants to crack a system

- I.e., break into a system
- Usually with malicious intent



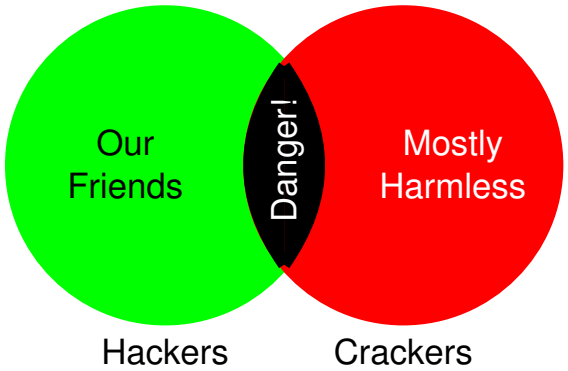
Some Terminology

hacker : someone who knows a lot about systems

- In particular, how they work
- Usually are programmers

cracker : someone who wants to crack a system

- I.e., break into a system
- Usually with malicious intent



- Reality is not so clear–cut
- Let's examine the "Crackersphere" . . .

The Crackersphere

- Crackers have different amounts of knowledge
- Crackers have different amounts of available resources
- Crackers have different motivations

The Crackersphere

- Crackers have different amounts of knowledge
- Crackers have different amounts of available resources
- Crackers have different motivations

- This means: some crackers are easier to prevent than others

The Crackersphere

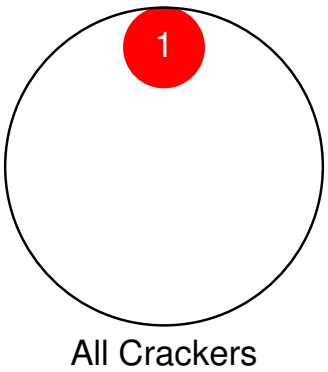
- Crackers have different amounts of knowledge
- Crackers have different amounts of available resources
- Crackers have different motivations

- This means: some crackers are easier to prevent than others

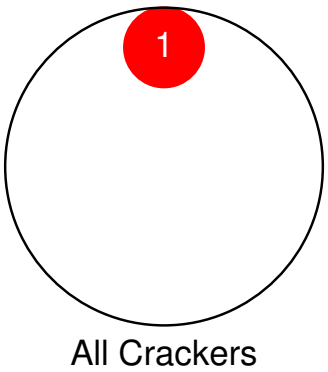
- Next: a breakdown into groups by "prevention difficulty"

An arbitrary discretization of crackers into groups

1. Nation states, terrorists

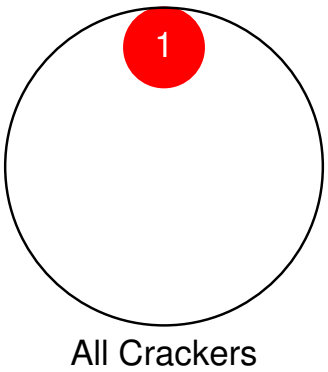


An arbitrary discretization of crackers into groups



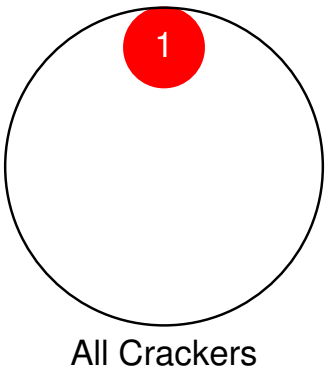
1. Nation states, terrorists
   - Knowledge, resources: high
     - Well–funded and well–organized
     - May employ various system experts
     - Large knowledge base
     - May design and manufacture custom devices

An arbitrary discretization of crackers into groups



1. Nation states, terrorists
   - Knowledge, resources: high
     - Well–funded and well–organized
     - May employ various system experts
     - Large knowledge base
     - May design and manufacture custom devices
   - Motivation (examples)
     - Intelligence
     - Information terrorism
     - Espionage
     - Strategic cyber-attacks and sabotage

An arbitrary discretization of crackers into groups

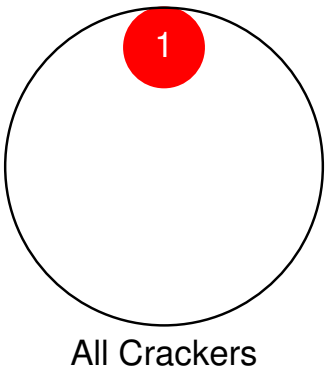


1. Nation states, terrorists
   - Knowledge, resources: high
     - Well–funded and well–organized
     - May employ various system experts
     - Large knowledge base
     - May design and manufacture custom devices
   - Motivation (examples)
     - Intelligence
     - Information terrorism
     - Espionage
     - Strategic cyber-attacks and sabotage

       Not science fiction

       E.g.: Stuxnet worm

An arbitrary discretization of crackers into groups



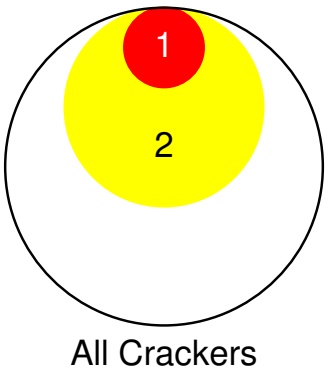
1. Nation states, terrorists
   - Knowledge, resources: high
     - Well–funded and well–organized
     - May employ various system experts
     - Large knowledge base
     - May design and manufacture custom devices
   - Motivation (examples)
     - Intelligence
     - Information terrorism
     - Espionage
     - Strategic cyber-attacks and sabotage

       Not science fiction

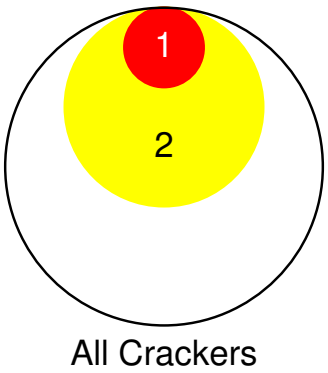
       E.g.: Stuxnet worm
   - Prevention difficulty: high

An arbitrary discretization of crackers into groups

2. Serious crackers

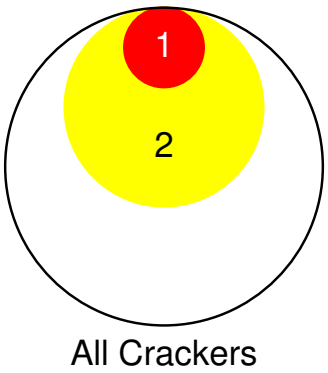


An arbitrary discretization of crackers into groups



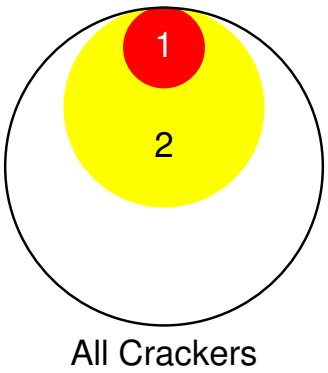
2. Serious crackers
   - Knowledge, resources: medium
     - Funded but limited
     - Knowledgeable about systems
     - May purchase devices
       E.g., keystroke loggers

An arbitrary discretization of crackers into groups



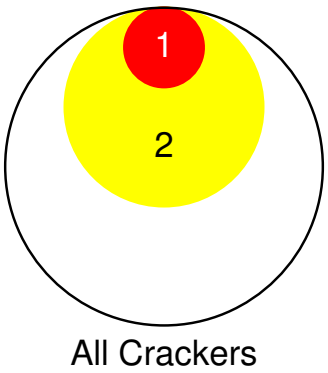
2. Serious crackers
   - Knowledge, resources: medium
     - Funded but limited
     - Knowledgeable about systems
     - May purchase devices
       E.g., keystroke loggers
   - Motivation (examples)
     - Civil disobedience
     - Selling secrets
     - Corporate espionage
     - Identity theft
     - Harassment
     - Embarassing organizations

An arbitrary discretization of crackers into groups



2. Serious crackers
   - Knowledge, resources: medium
     - Funded but limited
     - Knowledgeable about systems
     - May purchase devices
       E.g., keystroke loggers
   - Motivation (examples)
     - Civil disobedience
     - Selling secrets
     - Corporate espionage
     - Identity theft
     - Harassment
     - Embarassing organizations
       E.g.: Wikileaks, Murdoch hacking scandal

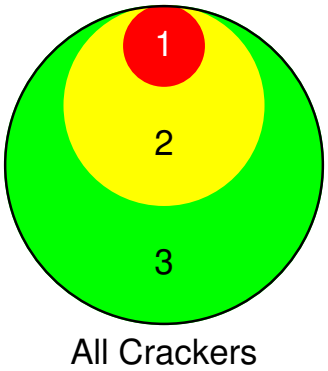
An arbitrary discretization of crackers into groups



2. Serious crackers
   - Knowledge, resources: medium
     - Funded but limited
     - Knowledgeable about systems
     - May purchase devices
       E.g., keystroke loggers
   - Motivation (examples)
     - Civil disobedience
     - Selling secrets
     - Corporate espionage
     - Identity theft
     - Harassment
     - Embarassing organizations
       E.g.: Wikileaks, Murdoch hacking scandal
   - Prevention difficulty: medium

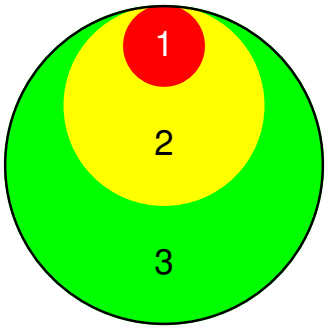
An arbitrary discretization of crackers into groups

3. Bottom feeders: script kids

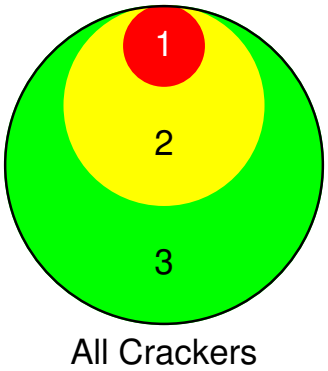


An arbitrary discretization of crackers into groups

3. Bottom feeders: script kids
   - Knowledge, resources: low to none
     - Know how to download and run scripts that some serious cracker has posted online

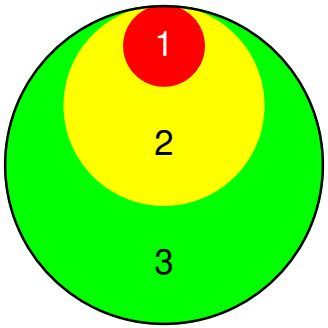


An arbitrary discretization of crackers into groups



3. Bottom feeders: script kids
   - Knowledge, resources: low to none
     - Know how to download and run scripts that some serious cracker has posted online
   - Motivation (examples)
     - Thrill seeking
     - Copycat attacks
     - "Street cred" with loser friends
     - Watched "Hackers" once to often
     - Too much free time

An arbitrary discretization of crackers into groups



3. Bottom feeders: script kids
   - Knowledge, resources: low to none
     - Know how to download and run scripts that some serious cracker has posted online
   - Motivation (examples)
     - Thrill seeking
     - Copycat attacks
     - "Street cred" with loser friends
     - Watched "Hackers" once to often
     - Too much free time
   - Prevention difficulty: easy
     - Because the script is available online, the vulnerability is already well–known
     - (Except maybe within a few days of posting)
     - You should have patched your system by now

Do you need to think about security?

Do you need to think about security?

1. Are your machines in your presence, or kept in a locked room, at all times?

Do you need to think about security?

1. Are your machines in your presence, or kept in a locked room, at all times?
2. Do you completely trust all users of the machines?

Do you need to think about security?

1. Are your machines in your presence, or kept in a locked room, at all times?
2. Do you completely trust all users of the machines?
3. Are your machines completely isolated from the outside?
   - Are all network connections to your own machines? And nobody ever connects a machine that goes outside?
   - Are all USB devices that are ever connected to your machines isolated from outside?

Do you need to think about security?

1. Are your machines in your presence, or kept in a locked room, at all times?
2. Do you completely trust all users of the machines?
3. Are your machines completely isolated from the outside?
   - Are all network connections to your own machines? And nobody ever connects a machine that goes outside?
   - Are all USB devices that are ever connected to your machines isolated from outside?

- If you answered "yes" to all questions
  - You are living in the first generation of computing (1940's and 1950's)
  - You may proceed without ever thinking about security
- If you answered "no" to *any* question — start being paranoid

Broad security topics

For the next lectures, anyway

- Physical security
- Authentication
- Authorization
- Network security
- Detecting intrusions

But first — System backups

- Not a security topic
  - Could be considered part of "data security"
- Are *relevant* for security
  - E.g., crackers may delete files

But first — System backups

- Not a security topic
  - Could be considered part of "data security"
- Are *relevant* for security
  - E.g., crackers may delete files

Flowchart for "do you need to think about backups"

But first — System backups

- Not a security topic
  - Could be considered part of "data security"
- Are *relevant* for security
  - E.g., crackers may delete files

Flowchart for "do you need to think about backups"

1. Do you care about any data on your system?

But first — System backups

- Not a security topic
  - Could be considered part of "data security"
- Are *relevant* for security
  - E.g., crackers may delete files

Flowchart for "do you need to think about backups"

1. Do you care about any data on your system?
2. Is that data stored on a device that could fail?

But first — System backups

- Not a security topic
  - Could be considered part of "data security"
- Are *relevant* for security
  - E.g., crackers may delete files

Flowchart for "do you need to think about backups"

1. Do you care about any data on your system?
2. Is that data stored on a device that could fail?

If yes to both — you need to have a backup plan

What to back up

What to back up

General rule: back up any data that would be hard to reconstruct

What to back up

General rule: back up any data that would be hard to reconstruct

- Definitely back up:
  - User files (`/home`)
  - Configuration files (`/etc` and `/var`)

What to back up

General rule: back up any data that would be hard to reconstruct

- Definitely back up:
  - User files (`/home`)
  - Configuration files (`/etc` and `/var`)
- Definitely do not back up:
  - `/tmp`, `/proc`, `/dev`

What to back up

General rule: back up any data that would be hard to reconstruct

- Definitely back up:
  - User files (`/home`)
  - Configuration files (`/etc` and `/var`)
- Definitely do not back up:
  - `/tmp`, `/proc`, `/dev`
- Grey area: other "system files"
  - E.g., kernel image, modules, libraries, applications?
  - Arguments for yes:
    - May be easier to rebuild the system
    - No danger of missing some critical file(s)
  - Arguments for no:
    - These things can be rebuilt "easily" by re-installing the OS
    - Backups will take more time and space if we include these

Types of backups

Types of backups

- Full backup
  - Make a copy of all files to be backed up

Types of backups

- Full backup
  - Make a copy of all files to be backed up
- Differential backup
  - Copy any file that has changed since the last full backup
  - Backups are usually faster than full
  - Recovery is usually slower than full

Types of backups

- Full backup
  - Make a copy of all files to be backed up
- Differential backup
  - Copy any file that has changed since the last full backup
  - Backups are usually faster than full
  - Recovery is usually slower than full
- Incremental backup
  - Copy any file that has changed since the last backup
  - Backups can be faster than differential
  - Recovery can be slower than differential

Types of backups

- Full backup
  - Make a copy of all files to be backed up
- Differential backup
  - Copy any file that has changed since the last full backup
  - Backups are usually faster than full
  - Recovery is usually slower than full
- Incremental backup
  - Copy any file that has changed since the last backup
  - Backups can be faster than differential
  - Recovery can be slower than differential

The terms “differential” and “incremental” are often confused

Typical backup media

- Magnetic tape
  - Very reliable
  - Easy to interchange tape cartridges
  - Recovery — slow to recover a single file
  - Tape drives can be expensive

Typical backup media

- Magnetic tape
  - Very reliable
  - Easy to interchange tape cartridges
  - Recovery — slow to recover a single file
  - Tape drives can be expensive
- Hard disk
  - Fairly reliable
  - Can be tough to interchange drives unless they are external
  - Generally more expensive per byte than tape cartridges

Typical backup media

- Magnetic tape
  - Very reliable
  - Easy to interchange tape cartridges
  - Recovery — slow to recover a single file
  - Tape drives can be expensive
- Hard disk
  - Fairly reliable
  - Can be tough to interchange drives unless they are external
  - Generally more expensive per byte than tape cartridges
- Optical media
  - Good long–term reliability
  - Infeasible for large backups

Typical backup media

- Magnetic tape
  - Very reliable
  - Easy to interchange tape cartridges
  - Recovery — slow to recover a single file
  - Tape drives can be expensive
- Hard disk
  - Fairly reliable
  - Can be tough to interchange drives unless they are external
  - Generally more expensive per byte than tape cartridges
- Optical media
  - Good long–term reliability
  - Infeasible for large backups
- Floppy disk, zip disk
  - Used prior to about 2000; is now dead technology. . .

Typical backup media

- Magnetic tape
  - Very reliable
  - Easy to interchange tape cartridges
  - Recovery — slow to recover a single file
  - Tape drives can be expensive
- Hard disk
  - Fairly reliable
  - Can be tough to interchange drives unless they are external
  - Generally more expensive per byte than tape cartridges
- Optical media
  - Good long–term reliability
  - Infeasible for large backups
- Floppy disk, zip disk
  - Used prior to about 2000; is now dead technology. . .
- Remote storage
  - Vendors provide secure and reliable storage
  - Performance depends on network

Backup utilities

`tar`

- Works great with tape, hard disk, and remote storage
- For optical: would need to "burn" the tarball to a disk
- Has options to archive files newer than a given date

Backup utilities

`tar`

- Works great with tape, hard disk, and remote storage
- For optical: would need to "burn" the tarball to a disk
- Has options to archive files newer than a given date

`rsync`

- Synchronizes data between two locations
- Can be used for hard disk and remote storage
- Smart — minimizes data transfer by only copying changes

Backup utilities: Macintosh

Time Machine

- Makes semi–regular full backups
- Makes regular incremental backups
- Can back up to any non–booting hard drive
- Easy to recover state of a file on any given date

Backup utilities: Windows

System Restore

- Only backs up certain system files
- Will create restore points
  - Does this before Windows updates and software installs, and at various other times
- Can roll back to earlier restore points

Windows backup

- Can create full and incremental backups
- Run the "backup wizard" to set this up

Backups — summary

- You should have some backup plan in place
- Can be a mixture of full and incremental backups; e.g.:
  - Full backups Sunday at 4am
  - Incremental backups Monday — Saturday at 4am
- Use automation to make this happen
  - Check out `cron` and `anacron` to do this yourself
- Check your backups occasionally
  - Make sure you can recover from them
- Consider off–site backups in your plan
  - Important for natural disasters
  - Remote storage is great for this
  - E.g., take an encrypted drive with a full backup of home machine to office every Monday

What is physical security?

What is physical security?

- In general — measures to deny physical access
  - E.g., locked doors, fences, cameras, security guards

What is physical security?

- In general — measures to deny physical access
  - E.g., locked doors, fences, cameras, security guards
- For sysadmins — also includes measures against crackers who have physical access
  - E.g., in public computer labs on campus

Single user mode

Must do all of the following to prevent crackers from booting in single user mode:

1. Use a GrUB password
   - Prevents editing of boot entries
2. Disable "boot from CD drive" in the BIOS
   - Prevents booting a live CD
3. Use a BIOS password
4. Lock machine(s) shut
   - Prevents crackers from resetting BIOS
   - Prevents crackers from changing drives

Theft

Private environments

Use locked doors, etc.

Theft

Private environments

Use locked doors, etc.

Public environments

- Use tie downs and locks
- These usually lock the machine shut also

Theft

Private environments

Use locked doors, etc.

Public environments

- Use tie downs and locks
- These usually lock the machine shut also

"Ha ha, thieves! Good luck guessing my password!"

Theft

Private environments

Use locked doors, etc.

Public environments

- Use tie downs and locks
- These usually lock the machine shut also

"Ha ha, thieves! Good luck guessing my password!"

- Is your machine locked shut? No?
  Then they can reset the BIOS and boot from a live CD...

Theft revisited

"Who is going to waste time stealing my ancient computer?"

Theft revisited

"Who is going to waste time stealing my ancient computer?"

- People after the data on your drive
  - Old tax returns
  - Credit card numbers
  - Amazon / eBay / Gmail / Facebook access
  - Music library

Theft revisited

"Who is going to waste time stealing my ancient computer?"

- People after the data on your drive
  - Old tax returns
  - Credit card numbers
  - Amazon / eBay / Gmail / Facebook access
  - Music library

Serious security breaches happen this way; e.g.:

- Company laptop stolen
- Laptop had database with millions of customers
  - Name, address, credit card

Theft revisited

"Who is going to waste time stealing my ancient computer?"

- People after the data on your drive
  - Old tax returns
  - Credit card numbers
  - Amazon / eBay / Gmail / Facebook access
  - Music library

Serious security breaches happen this way; e.g.:

- Company laptop stolen
- Laptop had database with millions of customers
  - Name, address, credit card

Encrypt any sensitive files!

Keyboard access

- If you step away from your machine you should
  - Log out; or
  - Lock the screen; or
    - Most modern screen savers can be configured to do this
  - Lock the office door
- It only takes a few seconds to
  - Install an ssh key
  - Delete your files
  - Read (or send) mail
- Some companies will fire you for leaving an unsecured machine

Keystroke loggers

- Record all keystrokes
  - Cracker will search for usernames and passwords
- Can be software–based
  - We need to prevent crackers from installing "system" software
    - Not just for keyloggers
    - We will discuss this later
- Can be hardware–based
  - Small and inexpensive
  - Not hard to build
  - Sit between keyboard and machine
  - Might be inside the keyboard
  - Need physical access to install
  - Need physical access to retrieve

A keystroke logger

Recap of authentication

Authentication: mechanism to prove that you are who you claim

- Knowledge factor: something you know
  - E.g., password, city of birth, name of first pet
  - Have issues...
- Possession factor: something you have
  - E.g., ATM card, certificates
- Inherence factor: something you are
  - E.g., fingerprint, iris scan

- Multi–factor authentication: uses two or more factors

How to crack a password

Two ways to attempt this

1. Online cracking
   - Attempt to crack the password through the actual system
     - Sit at a terminal and repeatedly try to login
     - Write a script to do this via ssh
   - A system can have countermeasures for this attack
     - Artificial delay
       e.g., it always takes 5 seconds to login
     - Lockout after repeated unsuccessful attempts
       e.g., after 5 failed attempts, no login for an hour
2. Offline cracking
   - Attempt to crack the password without going through system
   - Cracker must obtain hashed password(s) first
   - Compute hashes for each guess, until a match is found
     - See function `crypt()`
     - Easy to parallelize: 3 years using 1 machine can be done in one day using 1000 machines

Salt

Issue: a cracker could generate a database of hashed passwords

- Each entry: password and its hash
- This might take a while to build
- Can then simply "`grep`" a hash to find its matching password
- Could be sold to script kids for fun and profit

Salt

Issue: a cracker could generate a database of hashed passwords

- Each entry: password and its hash
- This might take a while to build
- Can then simply "`grep`" a hash to find its matching password
- Could be sold to script kids for fun and profit

Solution: use random salt

- A number of randomly–generated characters
- Are hashed with the password
- Salt can be determined from the hash
- Does not prevent use of a password database
  - But, multiplies the required size of the database
  - E.g., 24 bits of salt gives 16 million possible salt values
  - This makes a reverse–lookup database infeasible

Password space

Password space: set of all possible passwords

- Different systems allow different characters
- Different systems allow different lengths
- Password space grows with length and allowed characters

Allowed	**5 chars**	**6 chars**	**8 chars**
lower	$26^5 \approx 11 \times 10^6$	$26^6 \approx 308 \times 10^6$	$26^8 \approx 208 \times 10^9$
+ upper	$52^5 \approx 380 \times 10^6$	$52^6 \approx 19 \times 10^9$	$52^8 \approx 52 \times 10^{12}$
+ digits	$62^5 \approx 916 \times 10^6$	$62^6 \approx 56 \times 10^9$	$62^8 \approx 218 \times 10^{12}$
+ 32 special	$94^5 \approx 7 \times 10^9$	$94^6 \approx 689 \times 10^9$	$94^8 \approx 6 \times 10^{15}$

Password space

Password space: set of all possible passwords

- Different systems allow different characters
- Different systems allow different lengths
- Password space grows with length and allowed characters

Allowed	**5 chars**	**6 chars**	**8 chars**
lower	$26^5 \approx 11 \times 10^6$	$26^6 \approx 308 \times 10^6$	$26^8 \approx 208 \times 10^9$
+ upper	$52^5 \approx 380 \times 10^6$	$52^6 \approx 19 \times 10^9$	$52^8 \approx 52 \times 10^{12}$
+ digits	$62^5 \approx 916 \times 10^6$	$62^6 \approx 56 \times 10^9$	$62^8 \approx 218 \times 10^{12}$
+ 32 special	$94^5 \approx 7 \times 10^9$	$94^6 \approx 689 \times 10^9$	$94^8 \approx 6 \times 10^{15}$

- Brute force attack will check the entire password space
- Necessary to find random passwords
- But what if my password is not "random"?

Entropy — what is it?

- Information theory concept
- Idea: measure of "information content"
  - Number of bits required to store something
- Related to compression

1

Entropy — what is it?

- Information theory concept
- Idea: measure of "information content"
  - Number of bits required to store something
- Related to compression
- And how is this related to cracking passwords?

1

Entropy — what is it?

- Information theory concept
- Idea: measure of "information content"
  - Number of bits required to store something
- Related to compression
- And how is this related to cracking passwords?
- Password strength can be expressed in "entropy bits"
  - Effectively, log base 2 of the total search space where we are allowed to be very clever in our search

1

Entropy — what is it?

- Information theory concept
- Idea: measure of "information content"
  - Number of bits required to store something
- Related to compression
- And how is this related to cracking passwords?
- Password strength can be expressed in "entropy bits"
  - Effectively, log base 2 of the total search space where we are allowed to be very clever in our search
- Entropy examples

1

Entropy — what is it?

- Information theory concept
- Idea: measure of "information content"
  - Number of bits required to store something
- Related to compression
- And how is this related to cracking passwords?
- Password strength can be expressed in "entropy bits"
  - Effectively, log base 2 of the total search space where we are allowed to be very clever in our search
- Entropy examples
  - Number of 8–character dictionary words[1]: $30,000 \approx 2^{14.8}$

[1] Try `egrep '^.{8}$' /usr/share/dict/words | wc`

Entropy — what is it?

- Information theory concept
- Idea: measure of "information content"
  - Number of bits required to store something
- Related to compression
- And how is this related to cracking passwords?
- Password strength can be expressed in "entropy bits"
  - Effectively, log base 2 of the total search space where we are allowed to be very clever in our search
- Entropy examples
  - Number of 8–character dictionary words[1]: $30,000 \approx 2^{14.8}$ 14.8 bits of entropy
  - Number of 8–character random passwords: $26^8 \approx 2^{37.6}$

[1] Try `egrep '^.{8}$' /usr/share/dict/words | wc`

Entropy — what is it?

- Information theory concept
- Idea: measure of "information content"
  - Number of bits required to store something
- Related to compression
- And how is this related to cracking passwords?
- Password strength can be expressed in "entropy bits"
  - Effectively, log base 2 of the total search space where we are allowed to be very clever in our search
- Entropy examples
  - Number of 8–character dictionary words[1]: $30,000 \approx 2^{14.8}$ 14.8 bits of entropy
  - Number of 8–character random passwords: $26^8 \approx 2^{37.6}$ 37.6 bits of entropy

[1] Try `egrep '^.{8}$' /usr/share/dict/words | wc`

Smarter password cracking

Try a list of "likely" passwords

- Called a dictionary attack
- Start with dictionary words
- Add common substitutions, e.g.:
  - Changes in case
  - Letter "o" becomes number "0"
- Can put these in a file in order to try

Smarter password cracking

Try a list of "likely" passwords

- Called a dictionary attack
- Start with dictionary words
- Add common substitutions, e.g.:
  - Changes in case
  - Letter "o" becomes number "0"
- Can put these in a file in order to try

"But nobody is foolish enough to use that kind of password"

Smarter password cracking

Try a list of "likely" passwords

- Called a dictionary attack
- Start with dictionary words
- Add common substitutions, e.g.:
  - Changes in case
  - Letter "o" becomes number "0"
- Can put these in a file in order to try

"But nobody is foolish enough to use that kind of password"

- See `http://www.splashdata.com/press/PR121023.htm`
- Top 3 commonly–used passwords in 2012:

Smarter password cracking

Try a list of "likely" passwords

- Called a dictionary attack
- Start with dictionary words
- Add common substitutions, e.g.:
  - Changes in case
  - Letter "o" becomes number "0"
- Can put these in a file in order to try

"But nobody is foolish enough to use that kind of password"

- See `http://www.splashdata.com/press/PR121023.htm`
- Top 3 commonly–used passwords in 2012:
  1. password
  2. 123456
  3. 12345678

Strong passwords

- Are at least 8 characters
  - Use a passphrase if possible
- Contain a variety of character types
  - Upper, lower, digit, "special"
- Are not based on single words
- Are memorized
  - Or use a secure password manager
  - Are not written on a post it note stuck to your monitor
- Are changed regularly
- One way to select "more random" passwords:
  - Start with a sentence or phrase
  - Pull letters, symbols, and digits from it
  - Example:
    This semester, I will get 4 As produces `Ts,Iwg4A`
    Pretty good password and has a built–in expiration date

Avoiding weak passwords

- Some systems will not allow passwords based on a word
- Some systems will not allow short passwords
- For all VMs this semester
  - I had to set the password as `root`
  - Otherwise Linux complained that the passwords were too weak
- There are utilities
  - E.g., John the Ripper
    - Purpose is to detect weak passwords and notify users
    - Can also be used for evil

Other ways to get passwords

- Keystroke loggers

Other ways to get passwords

- Keystroke loggers
- Watch network traffic

Other ways to get passwords

- Keystroke loggers
- Watch network traffic
- Shoulder surfing
  - Watch over someone's shoulder

Other ways to get passwords

- Keystroke loggers
- Watch network traffic
- Shoulder surfing
  - Watch over someone's shoulder
- Listen to someone type their password
  - Different keys make different sounds
  - Google "Keyboard acoustic emanations"
  - `http://rakesh.agrawal-family.com/papers/ssp04kba.pdf`
  - This is an example of a side channel attack

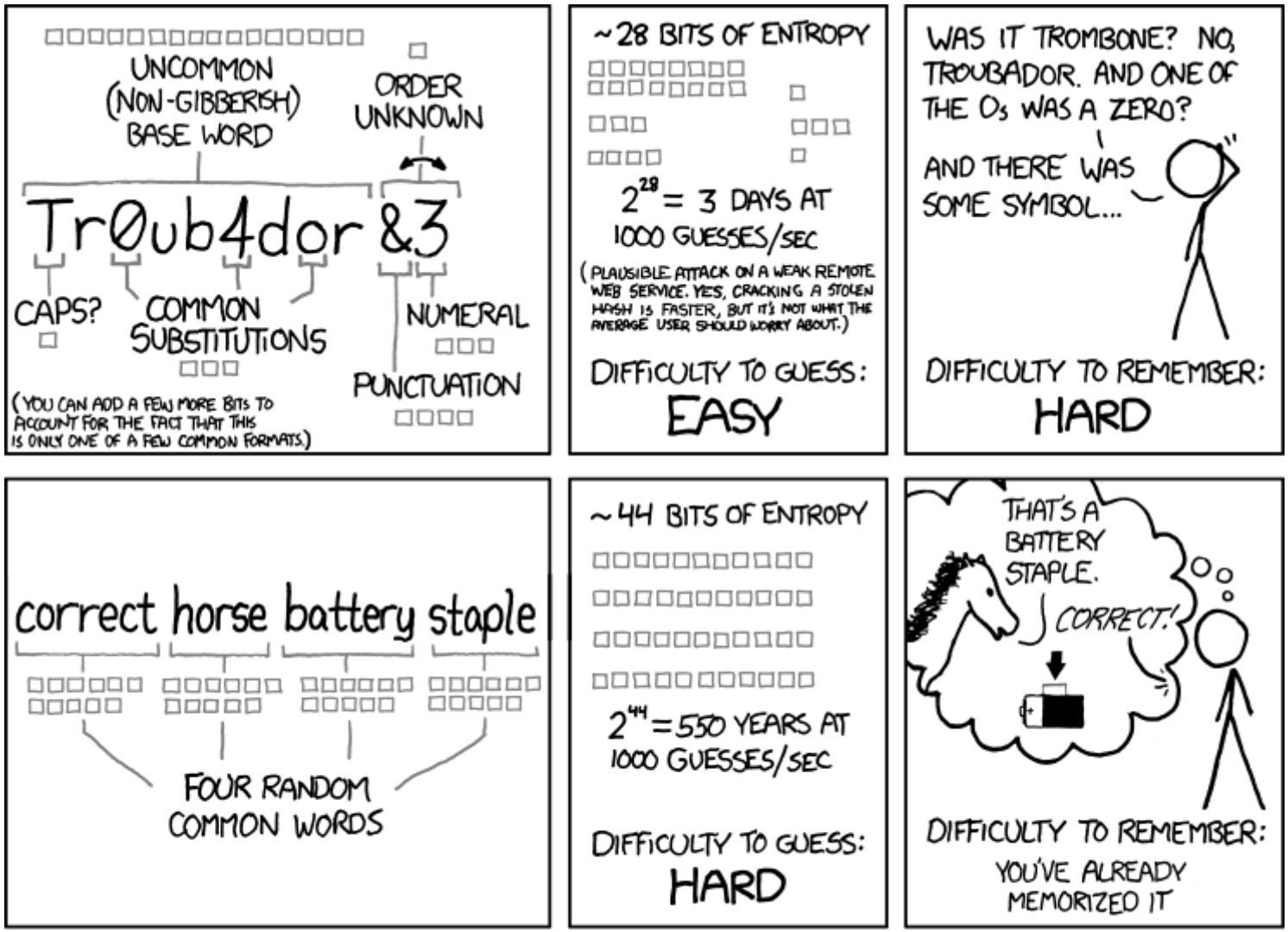
Other ways to get passwords

- Keystroke loggers
- Watch network traffic
- Shoulder surfing
  - Watch over someone's shoulder
- Listen to someone type their password
  - Different keys make different sounds
  - Google "Keyboard acoustic emanations"
  - `http://rakesh.agrawal-family.com/papers/ssp04kba.pdf`
  - This is an example of a side channel attack
- Crack a less secure system
  - People tend to re-use the same password (but shouldn't)
  - See `http://xkcd.com/792/`

Other ways to get passwords

- Keystroke loggers
- Watch network traffic
- Shoulder surfing
  - Watch over someone's shoulder
- Listen to someone type their password
  - Different keys make different sounds
  - Google "Keyboard acoustic emanations"
  - `http://rakesh.agrawal-family.com/papers/ssp04kba.pdf`
  - This is an example of a side channel attack
- Crack a less secure system
  - People tend to re-use the same password (but shouldn't)
  - See `http://xkcd.com/792/`
- Social engineering
  - Phishing is an example of this
  - Probably the most effective way to get passwords

Instructional xkcd comic: http://xkcd.com/936



End of lecture